On the Densest MIMO Lattices from Cyclic Division Algebras

Camilla Hollanti, Jyrki Lahtonen, *Member, IEEE*, Kalle Ranto, and Roope Vehkalahti

Abstract

It is shown why the discriminant of a maximal order within a cyclic division algebra must be minimized in order to get the densest possible matrix lattices with a prescribed nonvanishing minimum determinant. Using results from class field theory a lower bound to the minimum discriminant of a maximal order with a given center and index (= the number of Tx/Rx antennas) is derived. Also numerous examples of division algebras achieving our bound are given. E.g. we construct a matrix lattice with QAM coefficients that has 2.5 times as many codewords as the celebrated Golden code of the same minimum determinant. We describe a general algorithm due to Ivanyos and Rónyai for finding maximal orders within a cyclic division algebra and discuss our enhancements to this algorithm. We also consider general methods for finding cyclic division algebras of a prescribed index achieving our lower bound.

Index Terms

Cyclic division algebras, dense lattices, discriminants, Hasse invariants, maximal orders, multiple-input multiple-output (MIMO) channels, multiplexing, space-time block codes (STBCs).

I. Overview

Multiple-antenna wireless communication promises very high data rates, in particular when we have perfect channel state information (CSI) available at the receiver. In [1] the design criteria for such systems were developed, and further on the evolution of space-time (ST) codes took two directions: trellis codes and block codes. Our work concentrates on the latter branch.

We are interested in the coherent multiple input-multiple output (MIMO) case. A *lattice* is a discrete finitely generated free abelian subgroup $\mathbf{L}$ of a real or complex finite dimensional vector space $\mathbf{V}$, called the ambient space. In the space-time setting a natural ambient space is the space $\mathcal{M}_n(\mathbf{C})$ of complex $n \times n$ matrices. We only consider full rank lattices that have a basis $x_1, x_2, \ldots, x_{2n^2}$ consisting of matrices that are linearly independent over the field of real numbers. We can form a $2n^2 \times 2n^2$ matrix M having rows consisting of the real and imaginary parts of all the basis elements. It is well known that the measure, or hypervolume, $m(\mathbf{L})$ of the fundamental parallelotope of the lattice then equals the absolute value of $\det(M)$. Alternatively we may use the *Gram matrix*

$$G(\mathbf{L}) = MM^T = \left(\Re tr(x_i x_j^H)\right)_{1\leq i,j\leq 2n^2},$$

where H indicates the complex conjugate transpose of a matrix. The Gram matrix then has a positive determinant equal to $m(\mathbf{L})^2$.

From the pairwise error probability (PEP) point of view [2], the performance of a space-time code is dependent on two parameters: *diversity gain* and *coding gain*. Diversity gain is the minimum of the rank of the difference matrix $X - X'$ taken over all distinct code matrices $X, X' \in \mathcal{C}$, also called the *rank* of the code $\mathcal{C}$. When $\mathcal{C}$ is full-rank, the coding gain is proportional to the determinant of the matrix

This work was supported in part by the Nokia Foundation, the Foundation of Technical Development, Finland, the Foundation of the Rolf Nevanlinna Institute, Finland, and the Academy of Finland, grant #108238.

C. Hollanti and R. Vehkalahti are with the Laboratory of Discrete Mathematics for Information Technology, Turku Centre for Computer Science, Joukahaisenkatu 3-5 B, FIN-20520 Turku, Finland (e-mail: {cajoho, roiive}@utu.fi).

J. Lahtonen and K. Ranto are with the Department of Mathematics, FIN-20014 University of Turku, Finland (e-mail: {lahtonen, kara}@utu.fi).

$(X-X')(X-X')^H$. The minimum of this determinant taken over all distinct code matrices is called the *minimum determinant* of the code $\mathcal{C}$. If it is bounded away from zero even in the limit as SNR $\to \infty$, the ST code is said to have the *nonvanishing determinant* (NVD) property [3]. For non-zero square matrices, being full-rank coincides with being invertible.

The *data rate* R in symbols per channel use is given by

$$R = \frac{1}{n}\log_{|S|}(|\mathcal{C}|),$$

where $|S|$ and $|\mathcal{C}|$ are the sizes of the symbol set and code respectively. This is not to be confused with the *rate of a code design* defined as the ratio of the number of transmitted information symbols to the decoding delay (equivalently, block length) of these symbols at the receiver for any given number of transmit antennas using any complex signal constellations. If this ratio is equal to the delay, the code is said to have *full rate*.

The very first STBC for two transmit antennas was the *Alamouti code* [4] representing multiplication in the ring of quaternions. As the quaternions form a division algebra, such matrices must be invertible, i.e. the resulting STBC meets the rank criterion. Matrix representations of other division algebras have been proposed as STBCs at least in [5]-[14], and (though without explicitly saying so) [15]. The most recent work [7]-[15] has concentrated on adding multiplexing gain, i.e. multiple input-multiple output (MIMO) applications, and/or combining it with a good minimum determinant. It has been shown in [14] that CDA-based square ST codes with the NVD property achieve the diversity-multiplexing gain (D-MG) tradeoff introduced in [16]. The codes proposed in this paper all fall into this category and are in that sense optimal. Furthermore, algebras with an imaginary quadratic field as a center yield lattices with a good minimum determinant, as the corresponding rings of integers have no short non-zero elements.

Here, yet another design criterion is brought into the playground, namely an explicit criterion for maximizing the density of the code. The field of ST coding seems to be lacking a general, precise notion for the density in the case of noncommutative structures. In fact, according to our best knowledge the theory of orders required for giving this notion has never been considered before in this area.

Hence, after a cyclic division algebra has been chosen, the next step is to choose a corresponding lattice, or what amounts to the same thing, to choose an order within the algebra. Most authors [15], [14] have gone with the so-called natural order (see the next section for a definition). One of the points we want to emphasize in this article is to use the maximal orders instead. The idea is that one can sometimes use several cosets of the natural order without sacrificing anything in terms of the minimum determinant. So the study of maximal orders is clearly motivated by an analogy from the theory of error correcting codes: why one would use a particular code of a given minimum distance and length, if a larger code with the same parameters is available. The standard matrix representation of the natural order results in codes that have a so-called threaded layered structure [17]. When a maximal order is used, the code will then also extend ‘between layers’. However, our simulations suggest that restoring the layered structure somewhat by replacing the maximal order with its smartly chosen ideal yields codes with better performance. For more details about this see Section VII below. Earlier we have successfully used maximal orders in a construction of some 4Tx antenna MISO lattices [5].

In some cases the index of the natural order as a sublattice of a maximal order is quite large. E.g. in the cases of a family of cyclic algebras suggested in [11] one can theoretically increase the data rate by 1.5, 6.5 and 20.5 bits per channel use for 2, 4 and 8 antenna codes, respectively. We do emphasize that such increments of data rates are only theoretical in nature. This is because one is compelled to use relatively large subsets of the infinite lattice before the full density advantage of the maximal order is attained. Also the lattice of a fully multiplexing 8Tx+8Rx antenna MIMO code has dimension 128. The nearest vector problem in such high-dimensional lattices is used in some cryptographic applications, so it is safe to say that ML-decoding of such lattices will have prohibitive complexity. These numbers, however, motivated us to look for methods of locating maximal orders. A general purpose algorithm for this task has been developed by Ivanyos and Rónyai [18]. A commercially available version of their algorithm is implemented by W. van de Graaf as part of the computer algebra system MAGMA [19]. It turned out that this general purpose algorithm was not able to handle the algebras of index eight. To deal with these special cases we developed some enhancements to their algorithm.

Given that maximal orders provide the best codes in terms of minimum determinant vs. average power we are left with the question: Which division algebra should we use? To continue the analogy from the theory of error-correcting codes we want to find the codes with the highest possible density. That is, with the smallest fundamental parallelotope. To that end we need a suitable tool for parameterizing the cyclic division algebras with a given center and index. Luckily, relatively deep results from class field theory provide us with the necessary tool of Hasse invariants. The measure of a fundamental parallelotope of a maximal order (that will later on be referred to as the discriminant of the division algebra) can be expressed in terms of Hasse invariants [20]. With these results at hand we then derive a lower bound to the discriminant. While the proof of the lower bound is not constructive per se, it does show that our lower bound is achievable. In the latter parts of this article we describe some techniques for constructing division algebras with a minimal discriminant.

It is worth mentioning that in [21] the authors have made a similar approach in the reduced case of commutative number fields.

While our interest in these problems is mostly theoretical, some of the densest lattices we have found also perform well in computer simulations. Our construction of the densest 2×2 matrix lattice improves upon the deservedly celebrated Golden code in block error rates by about 0.9 dB at data rates from 5 to 6 bpcu. The performance of both the rival codes can be further improved by coset optimization and this also cuts down the gap to about 0.3 dB. Observe that at the data rate of 4 bpcu we have a tie. This is easily explained by the fact that for codes of that size there is a particularly attractive choice for the coset of the Golden code. Another point worth keeping in mind is that the somewhat irregular geometry of our lattice more or less necessitates the use of a code book as opposed to a simple combination of Gray coding and PAM. However, this also holds for the Golden code, when we do any coset optimization. Thus we might conclude that our work shows that not using a codebook costs about 1 dB.

The paper is organized as follows. In Section II, various algebraic notions related to cyclic algebras, Brauer groups, orders, discriminants, and localizations are introduced and demonstrated by examples. Furthermore, it is shown that maximizing the density of the code, i.e. minimizing the fundamental parallelotope is equivalent to minimizing the discriminant. This leads us to Section III, where we derive an achievable lower bound for the discriminant. In Section IV, we propose a general algorithm due to Ivanyos and Rónyai [18] for finding maximal orders. Unfortunately, when we were trying to use the MAGMA implementation of this algorithm for finding maximal orders of certain cyclic division algebra of index no more than 8, the memory of a typical modern PC turned out to be insufficient. Hence, also some enhancements to their algorithm in this special case are discussed here. The Perfect codes are analyzed in Section V in terms of Hasse invariants and discriminants. We show that the natural orders (i.e. the orders the authors have used in [10]) of the related algebras are maximal in the cases of $\#Tx = 2$ and $\#Tx = 3$, but can be enlarged in the cases of $\#Tx = 4$ and $\#Tx = 6$. In Section VI we construct division algebras with a minimal discriminant. The case of a unit non-norm element is separated from the general construction. Finally in Section VII, the theory is brought into practice by giving an explicit code construction that outperforms or ties with the Golden code. Simulation results are provided to back up this claim.

II. Cyclic algebras, Brauer groups, orders, and discriminants

We refer the interested reader to [22] and [7] for a detailed exposition of the theory of simple algebras, cyclic algebras, their matrix representations and their use in ST-coding. We only recall the basic definitions and notations here. In the following, we consider number field extensions E/F, where F denotes the base field and F^* (resp. E^*) denotes the set of the non-zero elements of F (resp. E). In the interesting cases F is an imaginary quadratic field, either $\mathbf{Q}(i)$ or $\mathbf{Q}(\sqrt{-3})$. We assume that E/F is a cyclic field extension of degree n with Galois group $\mathrm{Gal}(E/F) = \langle\sigma\rangle$. Let $\mathcal{A} = (E/F, \sigma, \gamma)$ be the corresponding cyclic algebra of degree n (n is also called the *index* of $\mathcal{A}$), that is

$$\mathcal{A} = E \oplus uE \oplus u^2E \oplus \cdots \oplus u^{n-1}E,$$

as a (right) vector space over E. Here $u \in \mathcal{A}$ is an auxiliary generating element subject to the relations $xu = u\sigma(x)$ for all $x \in E$ and $u^n = \gamma \in F^*$. An element $a = x_0 + ux_1 + \cdots + u^{n-1}x_{n-1} \in \mathcal{A}$ has the following representation as a matrix $A =$

$$\begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & & \gamma\sigma^{n-1}(x_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & & \gamma\sigma^{n-1}(x_3) \\ \vdots & & & & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix}.$$

We refer to this as the standard matrix representation of $\mathcal{A}$. Observe that some variations are possible here. E.g. one may move the coefficients γ from the upper triangle to the lower triangle by conjugating this matrix with a suitable diagonal matrix. Similarly one may arrange to have the first row to contain the "pure" coefficients $x_0, \ldots, x_{n-1}$. Such changes do not affect the minimum determinant nor the density of the resulting lattices.

If we denote the basis of E over $\mathcal{O}_F$ by $\{1, e_1, ..., e_{n-1}\}$, then the elements $x_i,\ i = 0, ..., n-1$ in the above matrix take the form $x_i = \sum_{k=0}^{n-1} f_k e_k$, where $f_k \in \mathcal{O}_F$ for all $k = 0, ..., n-1$. Hence n complex symbols are transmitted per channel use, i.e. the design has rate n. In literature this is often referred to as having a *full rate*.

Definition 2.1: The determinant (resp. trace) of the matrix A above is called the *reduced norm* (resp. *reduced trace*) of the element $a \in \mathcal{A}$ and is denoted by $nr(a)$ (resp. $tr(a)$).

Remark 2.1: The connection with the usual norm map $N_{\mathcal{A}/F}(a)$ (resp. trace map $T_{\mathcal{A}/F}(a)$) and the reduced norm $nr(a)$ (resp. reduced trace $tr(a)$) of an element $a \in \mathcal{A}$ is $N_{\mathcal{A}/F}(a) = (nr(a))^n$ (resp. $T_{\mathcal{A}/F}(a) = ntr(a)$), where n is the degree of E/F.

Definition 2.2: An algebra $\mathcal{A}$ is called *simple* if it has no nontrivial ideals. An F-algebra $\mathcal{A}$ is *central* if its center $Z(\mathcal{A}) = \{a \in \mathcal{A} \mid aa' = a'a\ \forall a' \in \mathcal{A}\} = F$.

Definition 2.3: Let S denote an arbitrary ring with identity. The *Jacobson radical* of the ring S is the set $\mathrm{Rad}(S) =$

$$\{x \in S \mid xM = 0 \text{ for all simple left } S\text{-modules } M\}.$$

$\mathrm{Rad}(S)$ is a two-sided ideal in S containing every nilpotent (i.e. for which $\mathcal{I}^k = 0$ for some $k \in \mathbf{Z}_+$) one-sided ideal $\mathcal{I}$ of S. Also, $\mathrm{Rad}(S)$ can be characterized as the intersection of the maximal left ideals in S. If S is a finite dimensional algebra over a field or, more generally, left or right Artinian then $\mathrm{Rad}(S)$ is the maximal nilpotent ideal in S.

A division algebra may be represented as a cyclic algebra in many ways as demonstrated by the following example.

Example 2.1: The division algebra $\mathcal{GA}$ used in [3] to construct the Golden code is gotten as a cyclic algebra with $F = \mathbf{Q}(i)$, $E = \mathbf{Q}(i, \sqrt{5})$, $\gamma = i$, when the F-automorphism σ is determined by $\sigma(\sqrt{5}) = -\sqrt{5}$. We also note that in addition to this representation $\mathcal{GA}$ can be given another construction as a cyclic algebra. As now $u^2 = i$ we immediately see that $F(u)$ is a subfield of $\mathcal{GA}$ that is isomorphic to the eighth cyclotomic field $E' = \mathbf{Q}(\zeta)$, where $\zeta = (1+i)/\sqrt{2}$. The relation $u\sqrt{5} = -\sqrt{5}u$ read differently means that we can view u as the complex number ζ and $\sqrt{5}$ as the auxiliary generator, call it $u' = \sqrt{5}$. We thus see that the cyclic algebra

$$E' \oplus u'E' = (E'/F, \sigma', \gamma')$$

is isomorphic to the Golden algebra. Here σ' is the F-automorphism of E' determined by $\zeta \mapsto -\zeta$ and $\gamma' = u'^2 = 5$.

Any cyclic algebra is a central simple F-algebra (cf. Definition 2.2). Two central simple F-algebras $\mathcal{A}$ and $\mathcal{B}$ are said to be *similar*, if there exist integers m an n such that the matrix algebras $\mathcal{M}_n(\mathcal{A})$ and $\mathcal{M}_m(\mathcal{B})$ are isomorphic F-algebras. Wedderburn's structure theorem [22, Theorem, p. 171] tells us that any central simple algebra is a matrix algebra over a central simple division algebra, and it easily follows that within any similarity class there is a unique division algebra. Similarity classes of central simple algebras form a group (under tensor product over F), called the *Brauer group* $\mathrm{Br}(F)$ of the field F. If F' is an extension field of F, and $\mathcal{A}$ is a central simple F-algebra, then the tensor product $\mathcal{A}' = \mathcal{A} \otimes_F F'$ is a central simple F'-algebra. We refer to this algebra as the algebra gotten from $\mathcal{A}$ by *extending the scalars to* F'.

The next proposition due to A. A. Albert [23, Theorem 11.12, p. 184] tells us when a cyclic algebra is a division algebra.

Proposition 2.1 (Norm condition): The cyclic algebra $\mathcal{A} = (E/F, \sigma, \gamma)$ of degree n is a division algebra if and only if the smallest factor $t \in \mathbf{Z}_+$ of n such that γ^t is the norm of some element of E^* is n.

Due to the above proposition, the element γ is often referred to as the *non-norm element*.

Let F be an algebraic number field that is finite dimensional over $\mathbf{Q}$. Denote its ring of integers by $\mathcal{O}_F$. If P is a prime ideal of $\mathcal{O}_F$, we denote the P-adic completion of F by $\hat{F}_P$. The division algebras over $\hat{F}_P$ are easy to describe. They are all gotten as cyclic algebras of the form $\mathcal{A}(n, r) = (E/\hat{F}_P, \sigma, \pi^r)$, where E is the unique unramified extension of $\hat{F}_P$ of degree n, σ is the Frobenius automorphism, and π is the prime element of F_P. The quantity r/n is called the *Hasse invariant* of this algebra and n is referred to as the *local index*. It immediately follows from Proposition 2.1 that $\mathcal{A}(n, r)$ is a division algebra, if and only if $(r, n) = 1$. For a description of the theory of Hasse invariants we refer the reader to [20, p. 266] or [24].

We are now ready to present some of the basic definitions and results from the theory of maximal orders. The general theory of maximal orders can be found in [20].

Let R denote a Noetherian integral domain with a quotient field F, and let $\mathcal{A}$ be a finite dimensional F-algebra.

Definition 2.4: An *R-order* in the F-algebra $\mathcal{A}$ is a subring Λ of $\mathcal{A}$, having the same identity element as $\mathcal{A}$, and such that Λ is a finitely generated module over R and generates $\mathcal{A}$ as a linear space over F. An order Λ is called *maximal*, if it is not properly contained in any other R-order.

Let us illustrate the above definition by concrete examples.

Example 2.2: (a) Orders always exist: If M is a *full* R-lattice in $\mathcal{A}$, i.e. $FM = \mathcal{A}$, then the *left order* of M defined as $\mathcal{O}_l(M) = \{x \in \mathcal{A} \mid xM \subseteq M\}$ is an R-order in $\mathcal{A}$. The right order is defined in an analogous way.

(b) If R is the ring of integers $\mathcal{O}_F$ of the number field F, then the ring of integers $\mathcal{O}_E$ of the extension field E is the unique maximal order in E. For example, in the case of the cyclotomic field $E = \mathbf{Q}(\zeta)$, where $\zeta = \exp(2\pi i/k)$ is a primitive root of order k the maximal order is $\mathcal{O}_E = \mathbf{Z}[\zeta]$.

The next proposition (see [26, proof of Theorem 3.2]) is useful when computing left orders in Section IV.

Proposition 2.2: Let $\mathcal{A}$ be a simple algebra over F and M a finitely generated $\mathcal{O}_F$-module such that $FM = \mathcal{A}$. Then there exists an element $s \in \mathcal{O}_F \setminus \{0\}$ such that $s \cdot 1 \in M$. Moreover, $\mathcal{O}_l(M) = \{b \in s^{-1}M \mid bM \leq M\} \leq s^{-1}M$.

For the purposes of constructing MIMO lattices the reason for concentrating on orders is summarized in the following proposition (e.g. [20, Theorem 10.1, p. 125]). We simply rephrase it here in the language of MIMO-lattices. We often (admittedly somewhat inaccurately) identify an order (or its subsets) with its standard matrix representation.

Proposition 2.3: Let Λ be an order in a cyclic division algebra $(E/F, \sigma, \gamma)$. Then for any non-zero element $a \in \Lambda$ its reduced norm $nr(a)$ is a non-zero element of the ring of integers $\mathcal{O}_F$ of the center F. In particular, if F is an imaginary quadratic number field, then the minimum determinant of the lattice Λ is equal to one.

Example 2.3: In any cyclic algebra we can always choose the element $\gamma \in F^*$ to be an algebraic integer. We immediately see that the $\mathcal{O}_F$-module

$$\Lambda = \mathcal{O}_E \oplus u\mathcal{O}_E \oplus \cdots \oplus u^{n-1}\mathcal{O}_E,$$

where $\mathcal{O}_E$ is the ring of integers, is an $\mathcal{O}_F$-order in the cyclic algebra $(E/F, \sigma, \gamma)$. We refer to this $\mathcal{O}_F$-order as the *natural order*. It will also serve as a starting point when searching for maximal orders.

We want the reader to note that in any central simple algebra a maximal **Z**-order is a maximal $\mathcal{O}_F$-order as well. Note also that if γ is not an algebraic integer, then Λ fails to be closed under multiplication. This may adversely affect the minimum determinant of the resulting matrix lattice, as elements not belonging to an order may have non-integral (and hence small) norms.

We remark that the term 'natural order' is somewhat misleading. While it is the first order that comes to mind, there is nothing canonical about it. Indeed, distinct realizations of a given division algebra as a cyclic algebra often lead to different natural orders. E.g. constructing the algebra of rational Hamiltonian quaternions from the cyclic extension $\mathbf{Q}(\sqrt{-3})/\mathbf{Q}$ as opposed to the more common $\mathbf{Q}(i)/\mathbf{Q}$ leads to a different natural order. The interested reader may verify this as an exercise by starting with the observation that the Hamiltonian quaternion $i + j + k$ may be used as a square root of -3.

Definition 2.5: Let $m = dim_F\mathcal{A}$. The *discriminant* of the R-order Λ is the ideal $d(\Lambda/R)$ in R generated by the set

$$\{\det(tr(x_i x_j))_{i,j=1}^m \mid (x_1, ..., x_m) \in \Lambda^m\}.$$

In the interesting cases of $F = \mathbf{Q}(i)$ (resp. $F = \mathbf{Q}(\sqrt{-3})$) the ring $R = \mathbf{Z}[i]$ (resp. $R = \mathbf{Z}[\omega]$, $\omega = (-1 + \sqrt{-3})/2$) is a Euclidean domain, so in these cases (as well as in the case $R = \mathbf{Z}$) it makes sense to speak of the discriminant as an element of R rather than as an ideal. We simply pick a generator of the discriminant ideal, and call it the discriminant. Equivalently we can compute the discriminant as

$$d(\Lambda/R) = \det(tr(x_i x_j))_{i,j=1}^m,$$

where $\{x_1, \ldots, x_m\}$ is any R-basis of Λ. It is readily seen that whenever $\Lambda \subseteq \Gamma$ are two R-orders, then $d(\Gamma)$ is a factor of $d(\Lambda)$. The index $[\Gamma : \Lambda]$ is related to discriminants by the following lemma.

Lemma 2.4:

$$[R : d(\Lambda)R] = [\Gamma : \Lambda]^2[R : d(\Gamma)R]$$

Proof: [20, p.66] ■

It turns out (cf. [20, Theorem 25.3]) that all the maximal orders of a division algebra share the same discriminant that we will refer to as the discriminant of the division algebra. In this sense a maximal order has the smallest possible discriminant among all orders within a given division algebra, as all the orders are contained in the maximal one.

For an easy reference we also note the following basic formula for the discriminant of certain cyclotomic fields.

Proposition 2.5: Let $\zeta_\ell = \exp(2\pi i/2^\ell)$ be a complex primitive root of unity of order 2^ℓ, where $\ell \geq 2$ is an integer. Then $n = [\mathbf{Q}(\zeta_\ell) : \mathbf{Q}(i)] = 2^{\ell-2}$ and

$$d(\mathbf{Z}[\zeta_\ell]/\mathbf{Z}[i]) = (1 + i)^{2n(\ell-2)}.$$

The definition of the discriminant closely resembles that of the Gram matrix of a lattice, so the following results are unsurprising and probably well known. We include them for lack of a suitable reference.

Lemma 2.6: Assume that F is an imaginary quadratic number field and that 1 and θ form a **Z**-basis of its ring of integers R. Assume further that the order Λ is a free R-module (an assumption automatically satisfied, when R is a principal ideal domain). Then the measure of the fundamental parallelotope equals

$$m(\Lambda) = |\Im\theta|^{n^2}|d(\Lambda/R)|.$$

Proof: Let $A = (a_{ij})$ be an $n \times n$ complex matrix. We flatten it out into a $2 \times 2n^2$ matrix $L(A)$ by first forming a vector of length n^2 out of the entries (e.g. row by row) and then replacing a complex number z by a diagonal two by two matrix with entries z and z^* (= the usual complex conjugate of z). If A and B are two square matrices with n rows we can easily verify the identities

$$L(A)L(B)^H = \begin{pmatrix} tr(AB^H) & 0 \\ 0 & tr(A^H B) \end{pmatrix} \tag{1}$$

and

$$L(A)L(B^T)^T = \begin{pmatrix} tr(AB) & 0 \\ 0 & tr(AB)^* \end{pmatrix}. \tag{2}$$

Next let $\mathcal{B} = \{x_1, x_2, \ldots, x_{n^2}\}$ be an R-basis for Λ. We form the $2n^2 \times 2n^2$ matrix $L(\mathcal{B})$ by stacking the matrices $L(x_i)$ on top of each other. Similarly we get $R(\mathcal{B})$ by using the matrices $L(x_i^T)^T$ as 'column blocks'. Then by (2) the matrix $M = L(\mathcal{B})R(\mathcal{B})$ consists of two by two blocks of the form

$$L(x_i)L(x_j^T)^T = \begin{pmatrix} tr(x_i x_j) & 0 \\ 0 & tr(x_i x_j)^* \end{pmatrix}.$$

Clearly $\det R(\mathcal{B}) = \pm \det L(\mathcal{B})$, and $\det M = |d(\Lambda/R)|^2$, so we get

$$|d(\Lambda/R)| = |\det L(\mathcal{B})|.$$

Next we turn our attention to the Gram matrix. By our assumptions the set $\mathcal{B} \cup \theta\mathcal{B}$ is a $\mathbf{Z}$-basis for Λ. Let us denote

$$D = \begin{pmatrix} 1 & 1 \\ \theta & \theta^* \end{pmatrix}.$$

From the identities $\Re(xy^*) = (xy^* + x^*y)/2$ and

$$D \begin{pmatrix} x & 0 \\ 0 & x^* \end{pmatrix} = \begin{pmatrix} x & x^* \\ \theta x & \theta^* x^* \end{pmatrix}$$

together with (1) it follows that for any two $n \times n$ matrices A and B we have

$$\frac{1}{2}\left(DL(A)\right)\left(DL(B)\right)^H = \begin{pmatrix} \Re(tr(AB^H)) & \Re(tr(A(\theta B)^H) \\ \Re(tr(\theta AB^H)) & \Re(tr(\theta A(\theta B)^H)) \end{pmatrix}.$$

Therefore, if we denote by $D^{[n]}$ the $2n^2 \times 2n^2$ matrix having n^2 copies of D along the diagonal and zeros elsewhere, we get the following formula for the Gram matrix

$$G(\Lambda) = \frac{1}{2}\left(D^{[n]}L(\mathcal{B})\right)\left(D^{[n]}L(\mathcal{B})\right)^H.$$

Thus,

$$m(\Lambda) = \det G(\Lambda)^{1/2} = |\det L(\mathcal{B})| \left|\frac{1}{2}\det D\right|^{n^2}.$$

Our claim now follows from all these computations and the fact that $(\det D)/2 = (\theta^* - \theta)/2 = -\Im\theta$. ■

In the respective cases $F = \mathbf{Q}(i)$ and $F = \mathbf{Q}(\sqrt{-3})$ we have $\theta = i$ and $\theta = (-1+\sqrt{-3})/2$ respectively, so we immediately get the following two corollaries.

Corollary 2.7: Let $F = \mathbf{Q}(i), R = \mathbf{Z}[i]$, and assume that $\Lambda \subset (E/F, \sigma, \gamma)$ is an R-order. Then the measure of the fundamental parallelotope equals

$$m(\Lambda) = |d(\Lambda/\mathbf{Z}[i])|.$$

Example 2.4: When we scale the Golden code [3] to have a unit minimum determinant, all the 8 elements of its $\mathbf{Z}$-basis will have length $5^{1/4}$ and the measure of the fundamental parallelotope is thus 25. In view of all of the above this is also a consequence of the fact that the $\mathbf{Z}[i]$-discriminant of the natural order of the Golden algebra is equal to 25. As was observed in [25] the natural order happens to be maximal in this case, so the Golden code cannot be improved upon by enlarging the order within $\mathcal{GA}$.

Corollary 2.8: Let $\omega = (-1+\sqrt{-3})/2$, $F = \mathbf{Q}(\omega)$, $R = \mathbf{Z}[\omega]$, and assume that $\Lambda \subset (E/F, \sigma, \gamma)$ is an R-order. Then the measure of the fundamental parallelotope equals

$$m(\Lambda) = (\sqrt{3}/2)^{n^2} |d(\Lambda/\mathbf{Z}[\omega])|.$$

The upshot is that in both cases **maximizing the density of the code, i.e. minimizing the fundamental parallelotope, is equivalent to minimizing the discriminant**. Thus, in order to get the densest MIMO-codes we need to look for division algebras that have a maximal order with as small a discriminant as possible.

For an easy reference we also include the following result that is a relatively easy consequence of the definitions.

Lemma 2.9: Let E/F be as above, assume that γ is an algebraic integer of F, and let Λ be the natural order of Example 2.3. If $d(E/F)$ is the $\mathcal{O}_F$-discriminant of $\mathcal{O}_E$ (often referred to as the relative discriminant of the extension E/F), then

$$d(\Lambda/\mathcal{O}_F) = d(E/F)^n \gamma^{n(n-1)}.$$

Proof: In the expansion

$$\Lambda = \mathcal{O}_E \oplus u\mathcal{O}_E \oplus \cdots \oplus u^{n-1}\mathcal{O}_E$$

we see that $u^i\mathcal{O}_E$ and $u^j\mathcal{O}_E$ are orthogonal to each other with respect to the bilinear form given by the reduced trace except in the cases where $i+j \equiv 0 \pmod{n}$. Assume that $i+j$ is divisible by n for some i,j in the range $0 \le i,j < n$, and that $x_1,\ldots,x_n$ are elements of $\mathcal{O}_E$. Then the multiplication rules of the cyclic algebra imply that

$$\det(tr(u^i x_k u^j x_\ell))_{k,\ell=1}^n = \pm\det(u^{i+j} tr(x_k x_\ell))_{k,\ell=1}^n = \pm\gamma^\epsilon \det(tr(x_k x_\ell))_{k,\ell=1}^n,$$

where the exponent ϵ is equal to zero or n according to whether $i+j$ equals zero or n. The former case occurs only once and the latter case occurs exactly $n-1$ times. The claimed formula then follows. ■

Example 2.5: We use the notation from Proposition 2.5. In [11] Kiran and Rajan have shown that the family of cyclic algebras $\mathcal{A}_\ell = (\mathbf{Q}(\zeta_\ell)/\mathbf{Q}(i), \sigma(\zeta_\ell) = \zeta_\ell^5, 2+i)$, with $\ell \ge 3$, consists entirely of division algebras. Let $\Lambda_{nat,\ell}$ be the natural order of the algebra $\mathcal{A}_\ell$. We may now conclude from Lemma 2.9, Proposition 2.5, and Corollary 2.7 that

$$d(\Lambda_{\ell,nat}/\mathbf{Z}[i]) = (2+i)^{n(n-1)}(1+i)^{2n^2(\ell-2)},$$

and that

$$m(\Lambda_{nat,\ell})^2 = 2^{2n^2(\ell-2)}5^{n(n-1)}.$$

For instance, in the 2 antenna case $\ell = 3, n = 2$, we have $m(\Lambda_{nat,\ell}) = 80$, and thus the Golden code is denser than the corresponding lattice $\mathcal{A}_3$ of the same minimum determinant. However, the natural order of $\mathcal{A}_3$ is not maximal and we will return to this example later on.

In Section IV some facts from the local theory of orders are required. For the basic properties of localization the reader can turn to [22, Chapter 7] or [20, Chapters 1, 2]. For the proofs for the rest of this section, see [18] and [26].

If R is a Dedekind domain with a quotient field F, and P is a prime ideal in R, then the ring of quotients $R_P = (R/P)^{-1}R \subset F$ is a discrete valuation ring. For the R-lattices M in $\mathcal{A}$ the localization at P is defined as $M_P = R_P M \subset \mathcal{A}$. M_P is an R_P-lattice. Moreover, if M is a full (cf. Example 2.2) R-lattice in $\mathcal{A}$, then M_P is a full R_P-lattice in $\mathcal{A}$. To be more specific, let us define the ring $\mathbf{Z}_p$.

Definition 2.6: For a rational prime p let $\mathbf{Z}_p$ denote the ring

$$\mathbf{Z}_p = \{\frac{r}{s} \in \mathbf{Q} \mid r,s \in \mathbf{Z},\ gcd(p,s) = 1\}.$$

$\mathbf{Z}_p$ is a discrete valuation ring with the unique maximal ideal $p\mathbf{Z}_p$. If Λ is a $\mathbf{Z}$-order we use the notation $\Lambda_p = \mathbf{Z}_p\Lambda$.

We remark that one should not confuse the localization R_P with the ring of integers $\hat{R}_P$ of the P-adic completion. We use the caret to indicate a complete structure. This is somewhat non-standard in the case of $\mathbf{Z}_p$ that is nearly universally used to denote the complete ring of p-adic integers. We use $\hat{\mathbf{Z}}_p$ for the complete ring.

The next statement illustrates a simple but useful connection between the orders Λ and Λ_p.

Proposition 2.10: Let Λ be a **Z**-order in $\mathcal{A}$. The map $\Phi : x \mapsto x + p\Lambda_p$, $x \in \Lambda$ induces an isomorphism of the rings $\Lambda/p\Lambda \cong \Lambda_p/p\Lambda_p$.

Proposition 2.11: Let P be a prime ideal of the ring R. The residue class ring $\overline{\Lambda} = \Lambda/P\Lambda$ is an algebra with identity element over the residue class field $\overline{R} = R/P$ and $dim_F\mathcal{A} = dim_{\overline{R}}\overline{\Lambda}$. If $\phi : \Lambda \to \overline{\Lambda}$ is the canonical epimorphism, then $P\Lambda \subseteq \operatorname{Rad}(\Lambda) = \phi^{-1}\operatorname{Rad}(\overline{\Lambda})$ and ϕ induces a ring isomorphism $\Lambda/\operatorname{Rad}(\Lambda) \cong \overline{\Lambda}/\operatorname{Rad}(\overline{\Lambda})$. As a consequence, a left (or right) ideal $\mathcal{I}$ of Λ is contained in $\operatorname{Rad}(\Lambda)$ if and only if there exists a positive integer t such that $\mathcal{I}^t \subseteq P\Lambda$.

The following facts establish some practical connections between the local and global properties of orders.

Proposition 2.12: Let $\mathcal{A}$ be a simple algebra over F. Let P be a prime ideal of R, and Γ be an R-order in $\mathcal{A}$. Then

(i) Γ_P is an R_P-order in $\mathcal{A}$.

(ii) Γ is a maximal R-order in $\mathcal{A}$ if and only if Γ_P is a maximal R_P-order in $\mathcal{A}$ for every prime ideal P of R.

(iii) $d(\Gamma/R)_P = d(\Gamma_P/R_P)$.

Proposition 2.13: Let P be a prime ideal of R and Γ be an R-order such that Γ_P is not a maximal R_P-order. Then there exists an ideal $\mathcal{I} \geq P\Gamma$ of Γ for which $\mathcal{O}_l(\mathcal{I}) > \Gamma$.

Extremal orders and especially Proposition 2.15 below play a key role in the method for constructing maximal orders.

Definition 2.7: We say that Γ_P radically contains Λ_P if and only if $\Lambda_P \subseteq \Gamma_P$ and $\operatorname{Rad}(\Lambda_P) \subseteq \operatorname{Rad}(\Gamma_P)$. The orders maximal with respect to this partial ordering are called *extremal*. Maximal orders are obviously extremal.

Proposition 2.14: An R_P-order Λ_P is extremal if and only if $\Lambda_P = \mathcal{O}_l(\operatorname{Rad}(\Lambda_P))$.

Proposition 2.15: Let $\Lambda_P \subset \Gamma_P$ be R_P-orders in $\mathcal{A}$. Suppose that Λ_P is extremal and that Γ_P is minimal among the R_P-orders properly containing Λ_P. Then there exists an ideal $\mathcal{J}$ of Λ_P minimal among those containing $\operatorname{Rad}(\Lambda_P)$ such that $\mathcal{O}_l(\mathcal{J}) \supseteq \Gamma_P$.

III. Discriminant bound

Again let F be an algebraic number field that is finite dimensional over **Q**, $\mathcal{O}_F$ its ring of integers, P a prime ideal of $\mathcal{O}_F$ and $\hat{F}_P$ the completion. In what follows we discuss the size of ideals of $\mathcal{O}_F$. By this we mean that ideals are ordered by the absolute values of their norms to **Q**, so e.g. in the case $\mathcal{O}_F = \mathbf{Z}[i]$ we say that the prime ideal generated by $2+i$ is smaller than the prime ideal generated by 3 as they have norms 5 and 9, respectively.

The following relatively deep result from class field theory is the key for deriving the discriminant bound. Assume that the field F is totally complex. Then we have the *fundamental exact sequence of Brauer groups* (see e.g. [20] or [24])

$$0 \longrightarrow \operatorname{Br}(F) \longrightarrow \oplus \operatorname{Br}(\hat{F}_P) \longrightarrow \mathbf{Q}/\mathbf{Z} \longrightarrow 0. \tag{3}$$

Here the first nontrivial map is gotten by mapping the similarity class of a central division F-algebra $\mathcal{D}$ to a vector consisting of the similarity classes of all the simple algebras $\mathcal{D}_P$ gotten from $\mathcal{D}$ by extending the scalars from F to $\hat{F}_P$, where P ranges over all the prime ideals of $\mathcal{O}_F$. Observe that $\mathcal{D}_P$ is not necessarily a division algebra, but by Wedderburn's theorem [22, p. 203] it can be written in the form

$$\mathcal{D}_P = \mathcal{M}_{\kappa_P}(\mathcal{A}_P),$$

where $\mathcal{A}_P$ is a division algebra with a center $\hat{F}_P$, and κ_P is a natural number called the *local capacity*. The second nontrivial map of the fundamental exact sequence is then simply the sum of the Hasse invariants of the division algebras $\mathcal{A}_P$ representing elements of the Brauer groups $\mathrm{Br}(\hat{F}_P)$.

This exact sequence tacitly contains the piece of information that for all but finitely many primes P the resulting algebra $\mathcal{D}_P$ is actually in the trivial similarity class of $\hat{F}_P$-algebras. In other words $\mathcal{D}_P$ is isomorphic to a matrix algebra over $\hat{F}_P$. More importantly, the sequence tells us that the sum of the nontrivial Hasse invariants of any central division algebras must be an integer. Furthermore, this is the only constraint for the Hasse invariants, i.e. any combination of Hasse invariants (a/m_P) such that only finitely many of them are non-zero, and that they sum up to an integer, is realized as a collection of the Hasse invariants of some central division algebra $\mathcal{D}$ over F.

Let us now suppose that with a given number field F we would like to produce a division algebra $\mathcal{A}$ of a given index n, having F as its center and the smallest possible discriminant. We proceed to show that while we cannot give an explicit description of the algebra $\mathcal{A}$ in all the cases, we can derive an explicit formula for its discriminant.

Theorem 3.1: Assume that the field F is totally complex and that $P_1, \dots, P_n$ are some prime ideals of $\mathcal{O}_F$. Assume further that a sequence of rational numbers $a_1/m_{P_1}, \dots, a_n/m_{P_n}$ satisfies

$$\sum_{i=1}^{n} \frac{a_i}{m_{P_i}} \equiv 0 \pmod 1,$$

$1 \leq a_i \leq m_{P_i}$, and $(a_i, m_{P_i}) = 1$.

Then there exists a central division F-algebra $\mathcal{A}$ that has local indices m_{P_i} and the least common multiple (LCM) of the numbers $\{m_{P_i}\}$ as an index.

If Λ is a maximal $\mathcal{O}_F$-order in $\mathcal{A}$, then the discriminant of Λ is

$$d(\Lambda/\mathcal{O}_F) = \prod_{i=1}^{n} P_i^{(m_{P_i}-1)\frac{[\mathcal{A}:F]}{m_{P_i}}}.$$

Proof: By exactness of the sequence (3) we know that there exists a central division algebra $\mathcal{A}$ over F which has local indices m_{P_i}. From [20, Theorem 32.19] we know that $\sqrt{[\mathcal{A}:F]} = LCM\{m_{P_i}\}$. By [20, Theorem 32.1] the discriminant then equals

$$d(\Lambda/R) = \left(\prod_{i=1}^{n} P_i^{(m_{P_i}-1)\kappa_{P_i}} \right)^{\sqrt{[\mathcal{A}:F]}}, \tag{4}$$

where κ_{P_i} is the local capacity.

A simple calculation of dimensions shows that

$$\kappa_P = \frac{\sqrt{[\mathcal{A}:F]}}{m_P}.$$

Substituting this into (4) we get the claim. ■

At this point it is clear that the discriminant $d(\Lambda)$ of a division algebra only depends on its local indices m_{P_i}.

Now we have an optimization problem to solve. Given the center F and an integer n we should decide how to choose the local indices and the Hasse invariants so that the LCM of the local indices is n, the sum of the Hasse invariants is an integer, and that the resulting discriminant is as small as possible. We immediately observe that at least two of the Hasse invariants must be non-integral.

Observe that the exponent $d(P)$ of the prime ideal P in the discriminant formula

$$d(P) = (m_P - 1)\frac{[\mathcal{A}:F]}{m_P} = n^2 \left(1 - \frac{1}{m_P} \right).$$

As for the nontrivial Hasse invariants $n \geq m_P \geq 2$, we see that $n^2/2 \leq d(P) \leq n(n-1)$. Therefore the nontrivial exponents are roughly of the same size. E.g. when $n = 6$, $d(P)$ will be either 18, 24 or 30 according to whether m_P is 2, 3 or 6. Not surprisingly, it turns out that the optimal choice is to have only two non-zero Hasse invariants and to associate these with the two smallest prime ideals of $\mathcal{O}_F$.

Theorem 3.2 (Main Theorem): Assume that F is a totally complex number field, and that P_1 and P_2 are the two smallest prime ideals in $\mathcal{O}_F$. Then the smallest possible discriminant of all central division algebras over F of index n is

$$(P_1 P_2)^{n(n-1)}.$$

Proof: By Theorem 3.1 the division algebra with Hasse invariants $1/n$ and $(n-1)/n$ at the primes P_1 and P_2 has the prescribed discriminant, so we only need to show that this is the smallest possible value.

By the above discussion it is clear that in order to minimize the discriminant one cannot have more than three nontrivial Hasse invariants. This is because for prime ideals P_1, P_2, P_3, P_4 (listed from the smallest to the largest) we always have

$$P_1^{d(P_1)} P_2^{d(P_2)} P_3^{d(P_3)} P_4^{d(P_4)} > (P_1 P_2)^{n(n-1)},$$

as the exponents $d(P_i) \geq n^2/2$ irrespective of the values of the Hasse invariants. A possibility is that some combination of three Hasse invariants might yield a smaller discriminant. Let us study this in detail.

If one of the local indices, say m_{P_1}, has only a single prime factor, say p, then we can add this Hasse invariant together with one of the other two, as long as we are careful to choose the one, say m_{P_2}, whose denominator is divisible by a smaller power of p. In this addition process the least common multiple of the denominators remains the same, so the new set of only two nontrivial Hasse invariants corresponds to a division algebra of the same index. This is because in the sum of the Hasse invariants

$$a_1/m_{P_1} + a_2/m_{P_2} = a'/m'_{P'} \pmod 1$$

the new local index $m'_{P'}$ is gotten from the old local index m_{P_2} by multiplying it with a (possibly the zeroth) power of p. Let P' be smaller of the two ideals P_1 and P_2. As $d(P_1)+d(P_2) > n(n-1) \geq d'(P')$, where $d'(P')$ is the exponent corresponding to the local index $m_{P'}$, this new division algebra (with nontrivial Hasse invariants associated with primes P' and P_3 only) will have a smaller discriminant.

The remaining case is that all the three local indices have at least two distinct prime factors. In this case all the three Hasse invariants have numerators ≥ 6. As then $d(P_1) + d(P_2) + d(P_3) > 2n(n-1)$, we see that the discriminant of the division algebra with these Hasse invariants also exceeds the stated lower bound. ■

We remark that in the most interesting (for MIMO) cases $n = 2$ and $n = 3$, the proof of Theorem 3.2 is more or less an immediate corollary of Theorem 3.1. We also remark that the division algebra achieving our bound is by no means unique. E.g. any pair of Hasse invariants $a/n, (n-a)/n$, where $0 < a < n$, and $(a, n) = 1$, leads to a division algebra with the same discriminant.

The smallest primes of the ring $\mathbf{Z}[i]$ are $1 + i$ and $2 \pm i$. They have norms 2 and 5 respectively. The smallest primes of the ring $\mathbf{Z}[\omega]$ are $\sqrt{-3}$ and 2 with respective norms 3 and 4. Together with Corollaries 2.7 and 2.8 we have arrived at the following bounds.

Corollary 3.3 (Discriminant bound): Let Λ be an order of a central division algebra of index n over the field $\mathbf{Q}(i)$. Then the measure of a fundamental parallelotope of the corresponding lattice

$$m(\Lambda) \geq 10^{n(n-1)/2}.$$

Corollary 3.4 (Discriminant bound): Let Λ be an order of a central division algebra of index n over the field $\mathbf{Q}(\omega)$, $\omega = (-1 + \sqrt{-3})/2$. Then the measure of a fundamental parallelotope of the corresponding lattice

$$m(\Lambda) \geq (\sqrt{3}/2)^{n^2} 12^{n(n-1)/2}.$$

The Golden algebra reviewed in Example 2.1 has its nontrivial Hasse invariants corresponding to the primes $2 + i$ and $2 - i$ and hence cannot be an algebra achieving the bound of Theorem 3.2. A clue for finding the optimal division algebra is hidden in the alternative description of the Golden algebra given in Example 2.1. It turns out that in the case $F=\mathbf{Q}(i)$, $E=\mathbf{Q}(\zeta)$ instead of using $\gamma'=5$ as in the case of the Golden algebra we can use its prime factor $\gamma=2+i$.

Proposition 3.5: The maximal orders of the cyclic division algebra $\mathcal{A}_3=(\mathbf{Q}(\zeta)/\mathbf{Q}(i),\sigma,2+i)$ of Example 2.5 achieve the bound of Theorem3.2.

Proof: The algebra $\mathcal{A}_3$ is generated as a $\mathbf{Q}(i)$-algebra by the elements ζ and u subject to the relations $\zeta^2=i$, $u^2=2+i$, and $u\zeta=-\zeta u$. The natural order $\mathbf{Z}[\zeta]\oplus u\mathbf{Z}[\zeta]$ is not maximal. Let us use the matrix representation of $\mathcal{A}_3$ as 2×2 matrices with entries in $\mathbf{Q}(\zeta)$, so elements of $\mathbf{Q}(i)$ are mapped to scalar matrices and ζ is mapped to a diagonal matrix with diagonal elements ζ and $-\zeta$. We observe that the matrix

$$w=\frac{1}{4}\begin{pmatrix} 2i-(1-i)\sqrt{2} & (2+i)(2i-(1+i)\sqrt{2}) \\ (1+i)(1+\sqrt{2}+i) & 2i+(1-i)\sqrt{2}\end{pmatrix}$$

is an element of $\mathcal{A}_3$. Straightforward calculations show that w satisfies the equations

$$w^2=-i+iw \quad \text{and} \quad w\zeta=-1+\zeta^3-\zeta w.$$

From these relations it is obvious that the free $\mathbf{Z}[\zeta]$-module with basis elements 1 and w is an order Λ. Another straightforward computation shows that $d(\Lambda/\mathbf{Z}[i])=-8+6i=(1+i)^2(2+i)^2$. As this is the bound of Theorem 3.2 we may conclude that Λ is a maximal order. ■

By Corollary 2.7 we see that the fundamental parallelotope of the maximal order in Proposition 3.5 has measure 10. Thus this code has 2.5 times the density of the Golden code.

The algebra $\mathcal{A}_3$ has the drawback that the parameter γ is quite large. This leads to an antenna power imbalance in both space and time domains. To some extent these problems can be alleviated by conjugating the matrix lattice by a suitable diagonal matrix (a trick used in at least [15]). One of the motifs underlying the perfect codes [10] is the requirement that the variable γ should have a unit modulus. To meet this requirement we proceed to give a different construction for this algebra.

Theorem 3.6: Let λ be the square root of the complex number $2+i$ belonging to the first quadrant of the complex plane. The cyclic algebra $\mathcal{GA}+=(\mathbf{Q}(\lambda)/\mathbf{Q}(i),\sigma,i)$, where the automorphism σ is determined by $\sigma(\lambda)=-\lambda$, is a division algebra. The maximal orders of $\mathcal{GA}+$ achieve the bound of Theorem 3.2. Furthermore, the algebras $\mathcal{GA}+$ and $\mathcal{A}_3$ of Theorem 3.5 are isomorphic.

Proof: The algebra $\mathcal{GA}+$ is a central algebra $F\{u',\lambda\}$ over the field $F=\mathbf{Q}(i)$ defined by the relations $\lambda^2=2+i$, $u'^2=i$, $u'\lambda=-\lambda u'$. Comparing these relations with the relations in the proof of Theorem 3.5 we get an isomorphism of F-algebras $f:\mathcal{GA}+\rightarrow\mathcal{A}_3$ by declaring $f(u')=\zeta$, $f(\lambda)=u$ and extending this in the natural way. The other claims follow immediately from this isomorphism and Theorem 3.5. ■

We refer to the algebra $\mathcal{GA}+$ as the *Golden+ algebra*. This is partly motivated by the higher density and partly by the close relation between the algebra $\mathcal{A}_3$ and the Golden algebra. After all, the algebra $\mathcal{A}_3$ comes out when in the alternative description of the Golden algebra (cf. Example 2.1) the variable $\gamma=5$ is replaced with its prime factor $2+i$. In Section IV we will provide an alternative proof for Theorem 3.6 by explicitly producing a maximal order within $\mathcal{GA}+$ and verifying that it has the prescribed discriminant. It is immediate from the discussion in the early parts of this section that in this case there is only one cyclic division algebra (up to isomorphism) with that discriminant.

It turns out that all the algebras $\mathcal{A}_\ell$ in the Kiran–Rajan family of Example 2.5 have maximal orders achieving the discriminant bound. The following observation is the key to prove this.

Lemma 3.7: Let F be either one of the fields $\mathbf{Q}(i)$ or $\mathbf{Q}(\omega)$, and let P_1 and P_2 be the two smallest ideals of its ring of integers R. Let $\mathcal{D}$ be a central division algebra over F, and let Λ be any R-order in $\mathcal{D}$. If the discriminant $d(\Lambda)$ is divisible by no prime other than P_1 and P_2, then any maximal order Γ of $\mathcal{D}$ achieves the discriminant bound of Theorem 3.2.

Proof: We know that there exists a maximal order, say Γ_0 containing Λ. The discriminant of Γ_0 is then a factor of $d(\Lambda)$, so P_1 and P_2 are the only prime divisors of $d(\Gamma_0)$. From Theorem 3.1 we infer that the only nontrivial Hasse invariants of $\mathcal{D}$ occur at P_1 and P_2. As the sum of the two Hasse invariants is an integer, they have the same denominator. This must then be equal to the index of $\mathcal{D}$. The discriminant formula of Theorem 3.1 then shows that $d(\Gamma_0)$ equals the discriminant bound. Any other maximal order in $\mathcal{D}$ shares its discriminant with Γ_0. ■

Corollary 3.8: Let $\ell > 2$ be an integer. The maximal orders of the cyclic division algebra $\mathcal{A}_\ell = (\mathbf{Q}(\zeta_\ell)/\mathbf{Q}(i), \sigma, 2+i)$ from Example 2.5 achieve the discriminant bound.

Proof: Proposition 2.5 and Lemma 2.9 indicate that the only prime factors of the discriminant of the natural order in $\mathcal{A}_\ell$ are $1+i$ and $2+i$. The claim then follows from Lemma 3.7. ■

At this point we remark that the natural orders of the algebras $\mathcal{A}_\ell$ of Example 2.5 are very far from being maximal. We will study this in greater detail in Section IV.

Example 3.1: Let $F = \mathbf{Q}(\sqrt{-3})$, so $\mathcal{O}_F = \mathbf{Z}[\omega]$. In this case the two smallest prime ideals are generated by 2 and $1-\omega$ and they have norms 4 and 3, respectively. By Theorem 3.2 the minimal discriminant is $4(1-\omega)^2$ when $n = 2$. As the absolute value of $1-\omega$ is $\sqrt{3}$ an application of the formula in Corollary 2.8 shows that the lattice $\mathbf{L}$ of the code achieving this bound has $m(\mathbf{L}) = 27/4$. In [27] we showed that a maximal order of the cyclic algebra $(E/F, \sigma(i) = -i, \gamma = \sqrt{-3})$, where $E = \mathbf{Q}(i, \sqrt{-3})$, achieves this bound.

We remark that one of the codes suggested in [15] is the natural order of the algebra of Example 3.1. However, the authors there never mentioned the possibility of using a maximal order. Nor did they mention that their lattice actually is an order.

IV. Finding maximal orders

Consider again the family of cyclic division algebras $\mathcal{A}_\ell$ of index $n = 2^{\ell-2}$ from Example 2.5. If Λ_ℓ is a maximal order of $\mathcal{A}_\ell$, then according to Corollary 3.8

$$d(\Lambda_\ell/\mathbf{Z}[i]) = (1+i)^{n(n-1)}(2+i)^{n(n-1)}.$$

On the other hand, by Example 2.5 we know that

$$d(\Lambda_{\ell,nat}/\mathbf{Z}[i]) = (1+i)^{2n^2(\ell-2)}(2+i)^{n(n-1)}.$$

Hence, by Lemma 2.4 we may conclude that the natural order is of index

$$[\Lambda_\ell : \Lambda_{\ell,nat}] = 2^{((2\ell-5)n+1)n/2}.$$

In the cases $\ell = 3, 4, 5$ this index thus equals 2^3, 2^{26}, and 2^{164}, respectively. In other words, using a maximal order as opposed to the natural order one can send 1.5, 6.5, or 20.5 more bits per channel use without compromising neither the transmission power nor the minimum determinant in the respective cases of 2, 4, or 8 antennas! Hence the problem of actually finding these maximal orders rather than simply knowing that they exist becomes quite relevant. In the following we shortly depict how maximal orders can be constructed in general. A more detailed version of the algorithm can be found in [18].

Let again F be an algebraic number field, $\mathcal{A}$ a finite dimensional central simple algebra over F, and Λ be a $\mathbf{Z}$-order in $\mathcal{A}$. Assume that $\mathcal{A}$ is given by relations (e.g. $u^2 = \gamma$), and that Λ is given by a $\mathbf{Z}$-basis. For instance, we can always start with the natural order Λ (cf. Example 2.3). We form a set $S = \{p_1, ..., p_r\}$ consisting of the rational primes dividing $d(\Lambda)$, i.e. Λ_p is a maximal $\mathbf{Z}_p$-order if $p \notin S$.

The basic idea of the algorithm is to test for $i = 1, ..., r$ whether Λ is maximal at p_i. If the answer is yes, Λ is a maximal $\mathbf{Z}$-order. If not, then at the first index i for which Λ_{p_i} is not maximal we can construct a $\mathbf{Z}$-order Γ in $\mathcal{A}$ such that $\Lambda_{p_i} \subset \Gamma_{p_i}$, and hence $\Lambda \subset \Gamma$ (cf. Propostitions 2.10–2.15). This can basically be done in two steps. Let $p \in S$.

STEP 1 REPEAT UNTIL “YES”: Compute $\mathcal{I} = \phi^{-1}(\mathrm{Rad}(\Lambda_p)) \leq \Lambda$. Does the equality $\mathcal{O}_l(\mathcal{I}) = \Lambda$ hold?

```
    “NO”: $\mathcal{O}_l(\mathcal{I}) \supset \Lambda$
        $\Lambda \leftarrow \mathcal{O}_l(\mathcal{I})$ (Iteration step)
```

STEP 2 REPEAT UNTIL "NO": Compute the minimal ideals $\mathcal{J}_1, \mathcal{J}_2, ..., \mathcal{J}_h$ ($h < dim_{\mathbf{Q}}\mathcal{A}$) of $\Lambda/p\Lambda$ which contain $\mathrm{Rad}(\Lambda/p\Lambda)$. FOR $i = 1, ..., h$ compute $\mathcal{I}_i = \phi^{-1}(\mathcal{J}_i)$. Does there exist an index i for which $\mathcal{O}_l(\mathcal{I}_i) > \Lambda$?

"YES": $\Lambda \leftarrow \mathcal{O}_l(\mathcal{I}_i)$ (Iteration step)

"NO": OUTPUT Λ is a maximal $\mathbf{Z}$-order.

Let $p \in S$. First we test whether Λ_p is an extremal (cf. Definition 2.7) $\mathbf{Z}_p$-order by checking if $\mathcal{O}_l(\mathrm{Rad}(\Lambda_p)) = \Lambda_p$. If not, then we shall construct a $\mathbf{Z}$-order $\Gamma > \Lambda$. If Λ_p passes this test, then we can use the test of Proposition 2.15. If there exists an ideal $\mathcal{J}$ minimal among the ideals properly containing $\mathrm{Rad}(\Lambda_p)$ such that $\mathcal{O}_l(\mathcal{J}) > \Lambda_p$, then we construct a $\mathbf{Z}$-order $\Gamma > \Lambda$. Otherwise we correctly conclude that Λ is maximal at p and continue with the next p in the list S. In the end, the algorithm yields a $\mathbf{Z}$-order Λ which is now maximal. The algorithm can be used similarly for constructing $\mathcal{O}_F$-orders, but in the MAGMA software the implementations are for $\mathbf{Z}$-orders only.

For more details concerning the computation of the prime ideals in a ring, see [26]. A thorough explanation and an algorithm for computing the radical can be found in [28].

Let us next exemplify the above algorithm.

A. 2×2 *construction over* $\mathbf{Z}[i]$

In the Golden division algebra (cf. Example 2.1 or [3]), i.e. the cyclic algebra $\mathcal{GA} = (E/F, \sigma, \gamma)$ gotten from the data $E = \mathbf{Q}(i, \sqrt{5})$, $F = \mathbf{Q}(i)$, $\gamma = i$, $n = 2$, $\sigma(\sqrt{5}) = -\sqrt{5}$, the natural order Λ is already maximal. The norm of the discriminant of Λ (with respect to $\mathbf{Q}$) is 625, whereas the norm of the minimal discriminant is 100 [27]. We will now present a code constructed from a maximal order of the cyclic division algebra $\mathcal{GA}+$ of Theorem 3.6. The maximal order of $\mathcal{GA}+$ also admits the minimal discriminant and is in that sense optimal. The algorithm now proceeds as follows.

The natural order of the algebra $\mathcal{GA}+$ is $\Lambda = \mathbf{Z}[i] \oplus u'\mathbf{Z}[i] \oplus \lambda\mathbf{Z}[i] \oplus u'\lambda\mathbf{Z}[i]$. Hereafter, we will use a shorter notation $\Lambda = \langle 1, u', \lambda, u'\lambda\rangle_{\mathbf{Z}[i]}$ for this. Let us consider Λ at the place $P = 1 + i$ as it is the only factor of the discriminant for which we can enlarge Λ. The inverse image of the radical (2.11) is $\mathcal{J} = \phi^{-1}(\mathrm{Rad}(\Lambda/P\Lambda)) = \phi^{-1}(\langle 1 + u', 1 + \lambda, 1 + u'\lambda\rangle_{\mathbf{Z}_2}) = \langle 1 + i, 1 + u', 1 + \lambda, 1 + u'\lambda\rangle_{\mathbf{Z}[i]} \subset \Lambda$. A straightforward computation shows us (cf. Proposition 2.2) that the element

$$\rho = \frac{1 + u' + \lambda + u'\lambda}{1 + i} = \frac{(1 + u')(1 + \lambda)}{1 + i} \in \mathcal{O}_l(\mathcal{J}),$$

which means that the answer to the question in Step 1 is "NO", and hence we set $\Lambda' = \langle 1, u', \lambda, \rho\rangle_{\mathbf{Z}[i]}$ and iterate. This time the inverse image of the radical is $\mathcal{J}' = \phi^{-1}(\mathrm{Rad}(\Lambda'/P\Lambda')) = \phi^{-1}(\langle 1 + u', 1 + \lambda, 1 + \rho\rangle_{\mathbf{Z}_2}) = \langle 1 + i, 1 + u', 1 + \lambda, 1 + \rho\rangle_{\mathbf{Z}[i]} \subset \Lambda'$. By taking the element

$$\tau = \frac{u' + \lambda}{1 + i} \in \mathcal{O}_l(\mathcal{J}')$$

we can again enlarge the order Λ' to $\Lambda'' = \langle 1, u', \tau, \rho\rangle_{\mathbf{Z}[i]}$ and compute $\mathcal{J}'' = \phi^{-1}(\mathrm{Rad}(\Lambda''/P\Lambda'')) = \phi^{-1}(\langle 1 + u', \tau, 1 + \rho\rangle_{\mathbf{Z}_2}) = \langle 1 + i, 1 + u', \tau, 1 + \rho\rangle_{\mathbf{Z}[i]} \subset \Lambda''$. We need one more iteration of Step 1. Now the element

$$\nu = \frac{(1 + u')(u' + \lambda)}{2} \in \mathcal{O}_l(\mathcal{J}'')$$

and the order Λ'' is enlarged to $\Lambda''' = \langle 1, \nu, \tau, \rho\rangle_{\mathbf{Z}[i]}$. From this iteration we finally get the answer to be "YES".

In Step 2 there is nothing to do, as the only minimal ideal properly containing the radical is the radical itself. Hence we have constructed a maximal $\mathbf{Z}[i]$-order of $\mathcal{GA}+$ with a $\mathbf{Z}[i]$-basis $\{1, \nu, \tau, \rho\}$.

In order to give a concrete description of this order we describe it in terms of its $\mathbf{Z}[i]$-basis. Let us again denote by λ the first quadrant square root of $2 + i$. The maximal order Λ consists of the matrices

$aM_1 + bM_2 + cM_3 + dM_4$, where a, b, c, d are arbitrary Gaussian integers and $M_i, i = 1, 2, 3, 4$ are the following matrices.

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad M_2 = \frac{1}{2}\begin{pmatrix} i+\lambda & i-i\lambda \\ 1+\lambda & i-\lambda \end{pmatrix}, \quad M_3 = \frac{1}{2}\begin{pmatrix} (1-i)\lambda & 1+i \\ 1-i & (i-1)\lambda \end{pmatrix},$$
$$M_4 = \frac{1}{2}\begin{pmatrix} (1-i)(1+\lambda) & (1+i)(1-\lambda) \\ (1-i)(1+\lambda) & (1-i)(1-\lambda) \end{pmatrix}.$$

B. Enhancements to the Ivanyos–Rónyai algorithm in some special cases

The memory requirements of the above algorithm grow quite rapidly as a function of the dimension of the algebra. E.g. the MAGMA-implementation runs out of memory on a typical modern PC, when given the index 8 cyclic algebra $\mathcal{A}_5$ of Example 2.5 as an input.

In this subsection we describe an algorithm that finds maximal orders for the algebras $\mathcal{A}_\ell$. It is an adaptation of the Ivanyos–Rónyai algorithm that utilizes several facts special to this family of algebras. We list these simple facts in the following lemmas. We will denote $\mathbf{Z}[\zeta_\ell]$ by $\mathcal{O}$ for short.

Lemma 4.1: The only prime ideal of $\mathcal{O}$ that lies above the prime 2 is the principal ideal P_ℓ generated by $1 - \zeta_\ell$.

Lemma 4.2: Let M be a finitely generated free $\mathcal{O}$-module of rank k, and let and $m_1, \ldots, m_k$ be a basis. Let N be a submodule of M such that the index $[M : N]$ is a power of two (in particular this index is finite). Then N is also a free $\mathcal{O}$-module of rank k, and we can find a basis of N of the form

$$n_i = \sum_{j \le i} a_{ij} m_j \quad , a_{ij} \in \mathcal{O}.$$

Proof: This is a straightforward modification of the proof of the corresponding result for modules over a PID. We briefly outline the argument, as we will need this later on. Let us start by choosing a basis $m_1, \ldots, m_k$ for M. We first consider the ideal I of those coefficients of m_k that appear in expansions of elements of N. We have a natural surjective homomorphism from M/N onto $\mathcal{O}/I$. Therefore the index of I in $\mathcal{O}$ is a power of two, so we may conclude that I is a power of the prime ideal P_ℓ. By Lemma 4.1 I is a principal ideal generated by a single element $y_k \in \mathcal{O}$. We may thus choose an element $n_k = y_k m_k + \sum_{i<k} x_i m_i$ from the submodule N. This will be the last element of a basis of N. We proceed by considering the submodule $N' = N \cap \sum_{i<k} \mathcal{O} m_i$ of vectors whose last coordinate vanishes. Then any element $n \in N$ can be written in the form $n = z_k n_k + n'$ where $n' \in N'$. The coefficients of m_{k-1} that appear in N' then again form an ideal that by the Jordan–Hölder theorem must be a power of P_ℓ, and the argument can be repeated. In the end we get a free $\mathcal{O}$-basis $n_1, n_2, \ldots, n_k$ of N such that

$$n_i = \sum_j b_{ij} m_j,$$

where all the coefficients $b_{ij} \in \mathcal{O}$, and $b_{ij} = 0$ whenever $j > i$. ■

Corollary 4.3: The maximal order Λ_ℓ of $\mathcal{A}_\ell$ is a free $\mathcal{O}$-module of rank $n = 2^{\ell-2}$.

Proof: We already know that Λ_ℓ contains $\Lambda_{\ell,nat}$ as a submodule of a finite index. Thus, there exists an integer $M > 0$ with the property that $M\Lambda_\ell$ is a submodule of finite index in $\Lambda_{\ell,nat}$. The formula for the discriminants tells us that we can further select the multiplier M to be a power of two. Clearly, it suffices to prove that $M\Lambda_\ell$ is a free module of the right rank. As the natural order, obviously, is a free $\mathcal{O}$-module of rank n, this is a consequence of Lemma 4.2. ■

Let then Γ be any *intermediate order*, i.e. any order with the property $\Lambda_{\ell,nat} \subseteq \Gamma \subseteq \Lambda_\ell$. We will denote by Γ_2 the ring gotten by localizing Γ at the prime $1 + i$. This is naturally a subring of the corresponding localized version of the maximal order and consequently also of the completion of the maximal order $\hat{\Lambda}_\ell$. This latter ring is a $\mathbf{Z}_2[i]$-order in the completion of the central simple $\mathbf{Q}_2(i)$-algebra $\hat{\mathcal{A}}_\ell$ gotten from $\mathcal{A}_\ell$ by extending its scalars to the complete field $\mathbf{Q}_2(i)$. Because the algebra $\mathcal{A}_\ell$ has a full local index $2^{\ell-2}$ at the prime $1+i$, $\hat{\mathcal{A}}_\ell$ is actually a division algebra. By [20, Theorem 12.8] and the surrounding discussion therein we know that $\hat{\Lambda}_\ell$ is a non-commutative discrete valuation ring, and that the $(1+i)$-adic valuation of the reduced norm serves as a valuation. E.g. it yields a metric subject to the non-archimedean triangle inequality. So in the matrix representation the valuation of the determinant distinguishes the units from the non-units in the ring $\hat{\Lambda}_\ell$. We immediately see that the same then holds in the ring Γ_2 — the units are precisely the elements whose reduced norm is a $(1+i)$-adic unit. By the non-archimedean triangle inequality the non-units of Γ_2 then form its unique maximal ideal, which is then also the radical $\mathrm{Rad}(\Gamma_2)$.

We summarize this line of reasoning in the following Lemma that is the key to our modifications to Step 1 in the main algorithm.

Lemma 4.4: Let Γ be any intermediate order. The ideal $\mathcal{I} = \Gamma \cap \mathrm{Rad}(\Gamma_2)$ consists of exactly those matrices which determinants are divisible by $1+i$.

The following lemma is a simple reformulation of the fact that P_ℓ is of index 2 in $\mathcal{O}$. It will allow us to reduce the range of certain searches from $\mathcal{O}$ to the set $\{0,1\}$.

Lemma 4.5: Assume that $p(x)=\sum_{i=0}^k p_i x^i \in \mathbf{Z}[x]$. Then

$$p(\zeta_\ell) \equiv p_0 + p_1 + \cdots + p_k \pmod{P_\ell}.$$

Let us denote by s_ℓ the complex number

$$s_\ell = \frac{1}{1-\zeta_\ell} = \frac{1+i}{2}\left(1+\zeta_\ell+\zeta_\ell^2+\cdots+\zeta_\ell^{n-1}\right).$$

The fractional ideal generated by s_ℓ is then P_ℓ^{-1}.

Proposition 4.6: Let Γ be an intermediate order. Assume that it is a free $\mathcal{O}$-module, and that $g_1, g_2, \ldots, g_n$ is its basis. Let $I = \phi^{-1}(\mathrm{Rad}(\Gamma_2))$ (cf. Step 1). Then I is also a free $\mathcal{O}$-module of rank n that satisfies $\Gamma \subseteq s_\ell I$. We can find a basis for I that is of the form $r_1, r_2, \ldots, r_n$, where for all i either

$$r_i = g_i + \sum_{j<i} \epsilon_{ij} g_j,$$

such that all the coefficients $\epsilon_{ij} \in \{0,1\}$, or

$$r_i = (1-\zeta_\ell) g_i.$$

Proof: Any element of Γ has determinant (= its reduced norm) in $\mathbf{Z}[i]$. The reduced norm of $1-\zeta_\ell$ is an associate of $1+i$. Therefore $(1-\zeta_\ell)\Gamma \subseteq I \subseteq \Gamma$. Thus the index of I in Γ is a power of two. Hence Lemma 4.2 implies that I is a free $\mathcal{O}$-module of rank n. With the notation of Lemma 4.2 we also see that the coefficient y_n is always either 1 or $1-\zeta_\ell$. In the former case Lemma 4.5 and the fact that $2 \in P_\ell$ allow us to choose the coefficients ϵ_{ij} as required. In the latter case we have no reason not to choose $r_i = (1-\zeta_\ell) g_i$ as this element is in I by Lemma 4.4. ■

Proposition 4.7: Let Γ, I, and the bases $g_1, \ldots, g_n$ and $r_1, \ldots, r_n$ be as in the previous proposition. Then the left order $\Gamma' = \mathcal{O}_\ell(I)$ is a free $\mathcal{O}$-module contained in $s_\ell \Gamma$. It has a basis $g_1', \ldots, g_n'$, where for all i either

$$g_i' = s_\ell(g_i + \sum_{j<i} \epsilon_{ij} g_j),$$

such that all the coefficients $\epsilon_{ij} \in \{0,1\}$, or

$$g_i' = g_i.$$

Proof: The inclusion $(1-\zeta_\ell)\Gamma \subseteq I$ immediately shows that $\Gamma \subseteq \mathcal{O}_\ell(I) \subseteq s_\ell \Gamma$. Therefore the index of $(1-\zeta_\ell)\Gamma'$ in Γ is a power of two. Again Lemma 4.2 shows that Γ' is a free $\mathcal{O}$-module. We also have the inclusion $(1-\zeta_\ell)\Gamma' \subseteq \Gamma$. An argument similar to the one in the proof of the previous proposition then shows that the algorithm in the proof of Lemma 4.2 yields a basis of the prescribed type. ■

When we use the natural order of the algebra $\mathcal{A}_\ell$ as a starting point, it is clear that $p = 1+i$ is the only interesting prime in Step 1 of the main algorithm. This step can now be completed simply by letting

Γ to be the natural order, and $g_1,\ldots,g_n$ to be its $\mathcal{O}$-module basis. We next find a basis for $\mathrm{Rad}(\Gamma)$ by testing, whether any element of the type $r_i = g_i + \sum_{j<i} \epsilon_{ij} g_j$ has a determinant divisible by $1+i$ (and if no such element is found then including $r_i = (1-\zeta_\ell) g_i$ into the basis instead). We then proceed to compute an $\mathcal{O}$-module basis for the left order Γ' of this $\mathrm{Rad}(\Gamma)$. Again we simply check, whether any elements of the form $g_i' = s_\ell(g_i + \sum_{j<i} \epsilon_{ij} g_j)$ belong to Γ'. Observe that it suffices to test a candidate of this form against the basis elements r_i only. If such an element is found, we record that Γ' will be strictly larger than Γ. If no such element is found, we use $g_i' = g_i$ instead. After we have done this for all i, we will know, whether $\Gamma' = \Gamma$. If this is the case, we are done. Otherwise we replace Γ with Γ' and repeat the process.

We implemented this on the computer algebra system Mathematica, and on a typical modern PC it found a maximal order in the case $\ell = 5$ in less than half an hour. We believe that the memory savings due to the use of $\mathcal{O}$-bases as opposed to $\mathbf{Z}$-bases in the general purpose implementation in MAGMA account for this enhancement in the performance of the algorithm. This algorithm could naturally be ported into any CAS to handle these very specific cases.

Example 4.1: Assume that we have the 4 antenna case $\ell = 4$. Let us denote $s = s_\ell$ for short. In this case the above algorithm yields an order with (left) $\mathcal{O}$-basis consisting of the elements $u_1,\ldots,u_4$:

$$\begin{aligned}
u_1 =& 1,\\
u_2 =& (s^2+s^3) + s^3 u,\\
u_3 =& (s^4+2s^5+2s^6+s^8+s^{10}) + (s^5+s^6)u + s^{10}u^2,\\
u_4 =& (s+s^4+s^5+s^8+s^9+s^{10}+s^{11}+s^{12}+s^{13}) + (s^9+s^{11}+s^{13})u + (s^{12}+s^{13})u^2 + s^{13}u^3.
\end{aligned}$$

We observe that the highest powers of s appearing in these basis elements are $0, 3, 10$, and 13, respectively. This fits well together with our earlier calculation showing that the index of the natural order in a maximal one is 2^{26}, as s^{-1} generates the prime ideal lying above 2, and $0+3+10+13=26$.

It is a basic fact from the theory of the cyclotomic rings of integers that the conjugate of the element s is of the form $\sigma(s) = u_\sigma s$, where u_σ is a unit of the ring $\mathbf{Z}[\zeta]$. Using this observation and the relation $us = \sigma(s)u$ we see that instead of the generator u_4 above we could use the product $u_2 u_3$. After all, the $\mathcal{O}$-module spanned by these elements is an order, so we can utilize the fact that it is closed under multiplication.

Example 4.2: In the 8 antenna case $\ell = 5$ we get a free $\mathcal{O}$-module of rank 8 as a maximal order. The basis elements $u_1,\ldots,u_8$ are similar linear combinations of $1, u, u^2, \ldots, u^7$ with coefficients of the form $p(s)$, where $p(x) \in \mathbf{Z}[x]$ and $s = s_\ell$. In this case the polynomial coefficients of the various basis elements have maximal degrees 0, 3, 10, 13, 28, 31, 38, and 41. As expected, these degrees sum up to 164. Taking advantage of the fact that this module is also a ring we can describe the elements of the basis by

$$\begin{aligned}
u_1 =& 1,\\
u_2 =& (s^2+s^3) + s^3 u,\\
u_3 =& (s+s^2+s^4+2s^5+2s^6+s^8+s^{10}) + (s^5+s^6)u + s^{10}u^2,\\
u_4 =& u_2 u_3,\\
u_5 =& s+2s^2+s^3+2s^4+5s^5+8s^6+8s^7+3s^8+5s^9+6s^{10}+5s^{11}\\
&+7s^{12}+6s^{13}+7s^{14}+4s^{15}+5s^{16}+2s^{18}+2s^{20}+s^{24}+s^{28}\\
&+\big(s^5+2s^6+4s^7+s^8+s^9+s^{10}+2s^{11}+2s^{12}+3s^{13}+3s^{14}+s^{15}+3s^{16}\big)u\\
&+\big(s^{11}+2s^{14}+2s^{15}+s^{16}+s^{18}+s^{20}\big)u^2+\big(s^{15}+s^{16}\big)u^3+s^{28}u^4,\\
u_6 =& u_2 u_5,\\
u_7 =& u_3 u_5,\\
u_8 =& u_2 u_3 u_5.
\end{aligned}$$

V. Analysis of the perfect algebras

In this section we illustrate some computational techniques related to Hasse invariants and discriminants. We use the algebras underlying the perfect codes as test cases, because this may provide some additional insight into these algebras. This section places somewhat higher demands on the readers' background in algebra and algebraic number theory. It may be skipped if desired, as our code construction will not depend on the material in this section.

Proposition 5.1: Let $\mathcal{D}_1 = (E_1/F, \sigma_1, \gamma_1)$ and $\mathcal{D}_2 = (E_2/F, \sigma_2, \gamma_2)$ be division algebras that have pairwise prime indices m_1 and m_2. Then $\mathcal{D}_1 \otimes \mathcal{D}_2$ is a division algebra with an index $m_1 m_2$. Further,

$$\mathcal{D}_1 \otimes \mathcal{D}_2 \simeq (E_1 E_2/F, \sigma_1\sigma_2, \gamma_1^{m_2}\gamma_2^{m_1}),$$

where $\sigma_1\sigma_2$ is an element of $\mathrm{Gal}(E_1E_2/F) \simeq \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F)$.

Let P_1 and P_2 be some pair of minimal prime ideals of the field F. If $\mathcal{D}_1$ and $\mathcal{D}_2$ have minimal discriminants that are only divisible by P_1 and P_2, then $\mathcal{D}_1 \otimes \mathcal{D}_2$ has a minimal discriminant that is only divisible by P_1 and P_2.

Proof: For the proof of the first two claims we refer the reader to [23, Theorem 20, p. 99]. The only nontrivial Hasse invariants of the division algebras $\mathcal{D}_1$ and $\mathcal{D}_2$ are those associated with primes P_1 and P_2. The mappings in the fundamental exact sequence (3) are homomorphisms of groups. Together with the fact that extending scalars to a P-adic completion commutes with the formation of a tensor product shows that the Hasse invariants of $\mathcal{D}_1 \otimes \mathcal{D}_2$ are sums of those of $\mathcal{D}_1$ and $\mathcal{D}_2$. Hence the discriminant of $\mathcal{D}_1 \otimes \mathcal{D}_2$ is only divisible by the prime ideals P_1 and P_2. By the proof of Theorem 3.2 it is then minimal. ■

Suppose we have a finite cyclic extension E/F of algebraic number fields. Let P be a prime of F and B some prime of E that lies over P. We denote the completion $\hat{E}_B$ by $\hat{E}_P$ or $E \cdot \hat{F}_P$. This notation is valid in Galois extensions, because the fields $\hat{E}_B$ are isomorphic for all primes B that lie over P.

A. 2×2 *perfect code*

The first perfect algebra is the same as the Golden algebra $\mathcal{GA} = (E/F, \sigma, \gamma)$, where the extension $E/F = \mathbf{Q}(i, \sqrt{5})/\mathbf{Q}(i)$ has discriminant $(2+i)(2-i)$. The discriminant of the natural order is therefore $(2+i)^2(2-i)^2$. Because the discriminant of the algebra $\mathcal{GA}$ divides $(2+i)^2(2-i)^2$ it can have at maximum two prime divisors $(2+i)$ and $(2-i)$. As a consequence the only Hasse invariants that can be nontrivial are $h_{(2+i)}$ and $h_{(2-i)}$.

The algebra $\mathcal{GA}$ must have at least two nontrivial Hasse invariants and therefore $h_{(2+i)}$ and $h_{(2-i)}$ are both nontrivial. Combining the equations LCM $[m_{(2+i)}, m_{(2-i)}] = 2$ and $h_{(2+i)} + h_{(2-i)} = 1$ we get that $h_{(2+i)} = h_{(2-i)} = 1/2$. Theorem 3.1 states that the discriminant of $\mathcal{GA}$ is $(2+i)^2(2-i)^2$. Comparing this to the discriminant of the natural order we see that the natural order is maximal.

B. 3×3 *perfect code*

The underlying algebra of the 3×3 perfect code is $\mathcal{P}_3 = (E/F, \sigma, \omega)$, where again $\omega = (-1+\sqrt{-3})/2$, $F = \mathbf{Q}(\omega)$, $E = \mathbf{Q}(\zeta_7 + \zeta_7^{-1}, \omega)$ and $\sigma : \zeta_7 + \zeta_7^{-1} \longmapsto \zeta_7^2 + \zeta_7^{-2}$. The algebra $\mathcal{P}_3$ has a representation as

$$L \oplus u \cdot L \oplus u^2 \cdot L$$

where $u^3 = \omega$.

The discriminant of the extension E/F is $(2+\sqrt{-3})^2(2-\sqrt{-3})^2 = P_1^2 P_2^2$ and the discriminant of the natural order has therefore only two prime factors. By Lemma 3.7 the only nontrivial Hasse invariants of $\mathcal{P}_3$ are h_{P_1} and h_{P_2}. Because LCM $[m_{P_1},\, m_{P_2}] = 3$. We get that $m_{P_1} = m_{P_2} = 3$.

To calculate the Hasse invariant h_{P_1} we pass to the completion $\mathcal{P}_{P_1} = \hat{F}_{P_1} \otimes \mathcal{P}_3$. From [20, Theorem 30.8] we get a cyclic representation $\mathcal{P}_{P_1} = (\hat{E}_{P_1}/\hat{F}_{P_1}, \sigma_{P_1}, \omega)$, where $\hat{E}_{P_1}/\hat{F}_{P_1}$ is a totally ramified extension and σ_{P_1} is the natural extension of the automorphism σ. Because the local index $m_{P_1} = 3$, we know that $\mathcal{P}_{P_1}$ is a division algebra.

Next we try to find another cyclic representation for this algebra so that we can use the definition of Hasse invariant to calculate the value of h_{P_1}.

It is readily verified that the field $\hat{F}_{P_1}(u) = T_{P_1} \subseteq \mathcal{P}_{P_1}$ is a cyclic and totally inert extension of $\hat{F}_{P_1}$. The Frobenius automorphism of the extension $\hat{T}_{P_1}/\hat{F}_{P_1}$ is defined by the $(\hat{T}_{P_1}/\hat{F}_{P_1}, P_1)(u) = u^7$. The Noether–Skolem Theorem ([20, Theorem 7.21]) states that there is an element $x \in \mathcal{P}_{P_1}$ such that

$$(\hat{T}_{P_1}/\hat{F}_{P_1}, P_1)(a) = x^{-1}ax \quad \forall a \in \hat{T}_{P_1}. \tag{5}$$

For an element x to fulfill (5) it is enough to satisfy the equation $(\hat{T}_{P_1}/\hat{F}_{P_1}, P_1)(u) = u^7 = xux^{-1}$. By considering the equation $ux = xu^7 = x\omega^2 u$ we see that $x = \zeta_7 + \zeta_7^{-1} + \omega^2(\zeta_7^2 + \zeta_7^{-2}) + \omega(\zeta_7^4 + \zeta_7^{-4}) \in L$ is a suitable element.

We now prove that x^3 is an element of F_{P_1}, and that $v_{P_1}(x^3) = 1$. The first statement follows from $u\sigma(x^3) = x^3u = x^2u\omega^2x = ux^3$. The second statement is obtained from the equation $v_{P_1}(x^3) = v_{P_1}(N_{E/F}(x)) = v_{P_1}(7(2 + (\sqrt{-3})\omega) = 1$.

Proposition 6.4 now states that $\mathcal{B}_1 = (\hat{T}_{P_1}/\hat{F}_{P_1}, (\hat{T}_{P_1}/\hat{F}_{P_1}, P_1), x^3)$ is a division algebra of index 3. By (5) we can consider $\mathcal{B}_1$ as a subset of the algebra $\mathcal{P}_3$. But $\mathcal{B}_1$ is a $\hat{F}_{P_1}$-central division algebra and hence a 9 dimensional vector space over $\hat{F}_{P_1}$. From this we can conclude that $(\hat{T}_{P_1}/\hat{F}_{P_1}, (\hat{T}_{P_1}/\hat{F}_{P_1}, P_1), x^3) = \mathcal{P}_{P_1}$.

Lemma 6.7 now implies that $h_{P_1} = 1/3$. Because the sum of the Hasse invariants has to be an integer, the invariant h_{P_2} is $2/3$.

By considering the local indices we see that the discriminant of the maximal order is $P_1^6 P_2^6$, that is, equal to the discriminant of the natural order. Thus, the natural order has to be maximal.

C. 4×4 *perfect code*

The division algebra under the 4×4 perfect code is $\mathcal{P}_4 = (E/F, \sigma, i)$, where $\mathbf{Q}(i) = F$, $\mathbf{Q}(i, \zeta_{15}+\zeta_{15}^{-1}) = E$ and $\sigma : \zeta_{15} + \zeta_{15}^{-1} \longmapsto \zeta_{15}^2 + \zeta_{15}^{-2}$.

The extension $E/\mathbf{Q}(i)$ has discriminant $d(E/\mathbf{Q}(i)) = (2+i)^3(2-i)^3(3)^2$, and the only Hasse invariants that can be nontrivial are $h_{(3)}, h_{(2+i)}$ and $h_{(2-i)}$. We use similar methods to those in the case of $\mathcal{P}_3$ to get that $h_{(2+i)} = 3/4$ and $h_{(2-i)} = 1/4$. The sum $h_{(2-i)} + h_{(2+i)} = 1$ and therefore $h_{(3)}$ must be trivial. Further, the local indices reveal that the discriminant of the algebra is $(2+i)^{12}(2-i)^{12}$. The discriminant of the natural order on the other hand is $(2+i)^{12}(2-i)^{12}(3)^8$. Lemma 2.4 tells us that the index of the natural order in the maximal order is 81.

D. 6×6 *perfect code*

In the 6×6 perfect code construction the center is $F = \mathbf{Q}(\omega)$ and the maximal subfield $E = K(\theta)$, where $\theta = \zeta_{28} + \zeta_{28}^{-1}$.

In [10] where the perfect codes were introduced, the authors gave the mapping σ_1 by the equation $\sigma_1 : \zeta_{28} + \zeta_{28}^{-1} \longmapsto \zeta_{28}^2 + \zeta_{28}^{-2}$. Unfortunately, this mapping is not an F-automorphism of the field E. We replace σ_1 with the automorphism σ defined by the equation $\sigma : \zeta_{28} + \zeta_{28}^{-1} \longmapsto \zeta_{28}^5 + \zeta_{28}^{-5}$. The relative discriminant of the extension E/F is $(2)^6(2 + \sqrt{-3})^5(2 - \sqrt{3})^5 = (2)^6(7)^5$. We denote the resulting algebra by $\mathcal{P}_6$.

Thus the Hasse invariants of $\mathcal{P}_6$ that can be nontrivial are $h_{(2+\sqrt{-3})}$, $h_{(2-\sqrt{-3})}$, and $h_{(2)}$.

Now we are going to present $\mathcal{P}_6$ as a product of two smaller division algebras. We first calculate the Hasse invariants of these smaller algebras and then from these derive the Hasse invariants of $\mathcal{P}_6$.

Let us first consider the algebra $\mathcal{B}_2 = (\mathbf{Q}(\sqrt{7}, \omega)/\mathbf{Q}(\omega), \sigma_2, -\omega)$. The algebra $\mathcal{B}_2$ is a division algebra with Hasse invariants $h_{(2-\sqrt{-3})} = h_{(2+\sqrt{-3})} = 1/2$. The proof is postponed until the end of Section VI.

The algebra $\mathcal{P}_3 = (E/F, \sigma_3, \omega)$ was previously shown to be a division algebra with Hasse invariants $h_{(2-\sqrt{-3})} = 2/3$ and $h_{(2+\sqrt{-3})} = 1/3$. We now consider the algebra $\mathcal{B}_3 = (E/F, \sigma_3, \omega^2)$. By [20, Theorem

30.4] we have $\mathcal{P}_3 \otimes \mathcal{B}_3 \sim (E/F, \sigma_3, 1) \simeq M_3(F)$. This shows that $\mathcal{P}_3 \otimes \mathcal{B}_3$ has trivial Hasse invariants and therefore the Hasse invariants of $\mathcal{B}_3$ are $h_{(2-\sqrt{-3})} = 1/3$ and $h_{(2+\sqrt{-3})} = 2/3$.

If we now consider the algebra $\mathcal{B}_3 \otimes \mathcal{B}_2 =$

$$(\mathbf{Q}(\sqrt{7}, \omega) \cdot \mathbf{Q}(\zeta_7 + \zeta_7^{-1}, \omega)/\mathbf{Q}(\omega), \sigma_2\sigma_3, (-\omega)^3 \cdot (\omega^2)^2)$$

it is seen that the corresponding Hasse invariants are $h_{(2-\sqrt{-3})} = 1/3 + 1/2 = 5/6$ and $h_{2+\sqrt{-3}} = 1/2 + 2/3 \equiv 1/6 \pmod 1$.

By considering the equation $\sigma_3(\zeta_7 + \zeta_7^{-1}) = \zeta_7^2 + \zeta_7^{-2} = \zeta_7^5 + \zeta_7^{-5}$ we notice that $\sigma_2\sigma_3 = \sigma_6$. Combining this and the equation $(-\omega)^3 \cdot \omega^4 = -\omega$ we get that $\mathcal{B}_3 \otimes \mathcal{B}_2 \simeq \mathcal{P}_6$.

The algebra $\mathcal{P}_6$ has only two nontrivial Hasse invariants that are $h_{(2+\sqrt{-3})} = 5/6$ and $h_{(2-\sqrt{-3})} = 1/6$. Whence, the discriminant of the maximal order is $(2-\sqrt{-3})^{30}(2+\sqrt{-3})^{30} = (7)^{30}$. The discriminant of the natural order on the other hand is $(2)^{36}(7)^{30}$. In this case Lemma 2.4 tells us that the perfect lattice is of relatively high index 2^{18} in its counterpart within the maximal order of same minimum determinant.

VI. Constructing division algebras with a minimal discriminant

We have divided this section into two parts. In the first part we are concentrating on algebras that have a cyclic representation with a unit non-norm element γ.

In the second section we relax the restriction on the size of γ and we give a general construction for $\mathbf{Q}(i)$ and $\mathbf{Q}(\sqrt{-3})$-central division algebras with a minimal discriminant.

One should note that none of the natural orders of the algebras we shall construct has a minimal discriminant. This, unfortunately, is not just a coincidence. In the following we prove that there are no natural orders reaching the bound of Theorem 3.2.

In the next lemma we use some basic results from the theory of discriminants and differents. For these results and the notion of different we refer the reader to [29, Chapter 3.12].

Lemma 6.1: Suppose we have a Galois extension E/F of degree n and that there are g prime ideals B_i of E lying over the prime P of F. If the prime P is wildly ramified in the extension E/F, then

$$v_P(d(E/F)) \geq n.$$

Proof: Suppose that $D_{E/F}$ is the different of the extension E/F. Then it is an easy exercise in Galois theory to show that $v_{B_i}(D_{E/F}) = v_{B_j}(D_{E/F})$ for every i and j. Because P was supposed to be wildly ramified

$$s = v_{B_i}(D_{E/F}) \geq e, \tag{6}$$

where e is the ramification index of B_i/P.

The theory of normal extension states that $efg = n$, where f is the inertial degree of B_i/P. Taking into account this and (6) we can conclude that

$$v_P(d(E/F)) = v_P(N_{E/F}(D_{E/F})) = sgf \geq egf = n.$$

■

Proposition 6.2: Suppose we have a division algebra $\mathcal{D} = (E/\mathbf{Q}(i), \sigma, \gamma)$, where $E/\mathbf{Q}(i) = n$ and γ is an algebraic integer. If Λ is the natural order of the division algebra $\mathcal{D}$, then

$$|d(\Lambda/\mathcal{O}_{\mathbf{Q}(i)})| > |(2+i)^{n(n-1))}(1+i)^{n(n-1)}|.$$

Proof: The natural order Λ is a subset of some maximal order Λ_{max} and therefore $|d(\Lambda/\mathcal{O}_{\mathbf{Q}(i)})| \geq |(2+i)^{n(n-1)}(1+i)^{n(n-1)}|$. Let us then assume that $|d(\Lambda/\mathcal{O}_{\mathbf{Q}(i)})| = |(2+i)^{n(n-1)}(1+i)^{n(n-1)}|$.

According to Lemma 2.9 the only primes that could be ramified in the extension $E/\mathbf{Q}(i)$ are $(1+i)$, $(2+i)$, and $(2-i)$. Lemma 6.1 assures that none of these primes could be wildly ramified.

One of the main results of the global class field theory [24, p. 124] states that there exists a ray class field $C_{(1+i)(2+i)(2-i)}$ that contains all the cyclic extensions of $\mathbf{Q}(i)$ where $(1+i)$, $(2+i)$, or $(2-i)$ is tamely ramified.

We can now calculate the degree of the extension $C_{(2+i)(1+i)(2-i)}/\mathbf{Q}(i)$. By [24, Theorem 1.5] we have $[C_{(2+i)(1+i)(2-i)} : \mathbf{Q}(i)] = 2$, which implies that $E = C_{(2+i)(1+i)(2-i)}$ and $n = 2$.

The ray class fields $C_{(2+i)(1+i)}$ and $C_{(2-i)(1+i)}$ that admit tame ramification at $(2+i)$ and $(1+i)$ or, at $(2+i)$ and $(1-i)$, respectively, are both trivial extensions of $\mathbf{Q}(i)$. Hence, both $(2+i)$ and $(2-i)$ are ramified in E and divide the discriminant of the extension $E/\mathbf{Q}(i)$. The discriminant of the natural order Λ now has to be divisible by at least $(2+i)^2(2-i)^2$. This gives us a contradiction. ■

Proposition 6.3: Suppose we have a division algebra $\mathcal{D} = (E/\mathbf{Q}(\sqrt{-3}), \sigma, \gamma)$, where $E/\mathbf{Q}(\sqrt{-3}) = n$ and γ is an algebraic integer. If Λ is the natural order of the division algebra $\mathcal{D}$, then

$$|d(\Lambda/\mathcal{O}_{\mathbf{Q}(\sqrt{-3})})| > |(\sqrt{-3})^{n(n-1))}(2)^{n(n-1)}|.$$

Proof: The proof is similar to that of the previous proposition. ■

These considerations reveal that reaching the optimal density of a code-lattice requires considering maximal orders instead of natural ones.

We give one simple lemma for later use, it is a slight generalization to [11, Theorem 1]. We denote the multiplicative ideal group of the field F by $(I_F)^*$.

Lemma 6.4: Let E be a Galois extension of a number field F and let P be a prime ideal of $\mathcal{O}_F$ that lies under the prime B of the ring $\mathcal{O}_E$. If the inertial degree of P in the extension E/F is f and γ is such an element of F that $(v_P(\gamma), f) = 1$, then $\gamma^i \notin N_{E/F}(E)$ for any $i = 1, 2, \dots, f-1$.

Proof: The ideal norm of B is $N_{E/F}(B) = P^f$, where f is the inertial degree of P in the extension E/F. It is clear that the group $N_{E/F}((I_F)^*)$ is generated by the norms of prime ideals and that $\{N_{E/F}(a)\mathcal{O}_F \mid a \in E^*\} \subseteq N_{E/F}(I_F)$. Therefore $f | v_P(N_{E/F}(a)\mathcal{O}_F)$ for all $a \in E$. ■

A. *Algebras with a unit γ*

TABLE I

$\mathbf{Q}(i)$-CENTRAL DIVISION ALGEBRAS WITH A UNIT γ

n	γ	f_n
2	i	$x^2 + (2+i)$
4	i	$x^4 + (2+i)$

1) Center $\mathbf{Q}(i)$: In Table I we give a cyclic representations for algebras of degree 2 and 4. Proposition 2.1 implies that 4 is the biggest degree that we can hope to have a cyclic division algebra with a unit γ. There does not exist such an algebra of degree 3. The reason for this is that in every cyclic extension $E/\mathbf{Q}(i)$ of degree three, all the units of $\mathbf{Q}(i)$ are third powers and therefore are in the image of the norm $N_{E/\mathbf{Q}(i)}$.

In the following we use the generic notation $\mathbf{Q}(i) = F$ and $E = F(a_n)$, where a_n is a zero of the polynomial f_n.

Algebra $\mathcal{D}_2$: The algebra $\mathcal{D}_2$ was previously shown to be a division algebra with a minimal discriminant.

Algebra $\mathcal{D}_4$: When considering $\mathcal{D}_4$ we first have to check whether it really is a division algebra. We note that $(2+i)$ is a totally ramified prime in E/F. This results in the local extension $E_{(2+i)}/F_{(2+i)}$ being a totally and tamely ramified cyclic extension of degree 4. We note that $\#(\mathcal{O}_{F_{(2+i)}}/(2+i)\mathcal{O}_{F_{(2+i)}}) = \#(\mathcal{O}_F/(2+i)) = 5$.

Proposition 2.1 states that $\mathcal{D}_4$ is a division algebra if i satisfies the norm condition, i.e. neither of the elements $\{i, -1\}$ is a norm.

Hasse Norm Theorem [20, Theorem 32.8] states that it is enough to show that the elements $\{i, -1\}$ are not norms in the extension $\hat{E}_{(2+i)}/\hat{F}_{(2+i)}$. Elementary local theory [30, Proposition 7.19] states that if we have any complete residue system $\{0, 1, a, b, c\}$ of the group $\mathcal{O}_{\hat{E}_{(2+i)}}/(2+i)\mathcal{O}_{\hat{E}_{(2+i)}}$ and an arbitrary unit $e \in \hat{F}_{(2+i)}$ then

$$\hat{E}^*_{2+i} = \{1, a, b, c\} \times (1 + (2+i)\mathcal{O}_{\hat{E}_{2+i}}) \times \langle e(2+i)\rangle. \tag{7}$$

The prime $(2+i)$ is tamely ramified in $\hat{E}_{(2+i)}/\hat{F}_{(2+i)}$ and therefore the *local conductor* is $(2+i)$ ([24, p. 12]). The definition of the conductor now implies that $(1 + (2+i)\mathcal{O}_{\hat{E}_{2+i}} \subseteq N_{\hat{E}_{(2+i)}/\hat{F}_{(2+i)}}(\hat{E}_{(2+i)})$. Because the prime $(2+i)$ is totally ramified, we have $e_1(2+i) \subseteq N_{\hat{E}_{(2+i)}/\hat{F}_{(2+i)}}(\hat{F}_{(2+i)})$ for some unit $e_1 \in \hat{F}_{(2+i)}$. The previous results now imply that $(1 + (2+i)\mathcal{O}_{\hat{E}_{(2+i)}}) \times \langle e_1(2+i)\rangle \subseteq N_{\hat{E}_{(2+i)}/\hat{F}_{(2+i)}}(\hat{E}_{2+i})$.

One of the main theorems of local class field theory states that $(\hat{F}_{(2+i)})^*/(N_{\hat{E}_{(2+i)}/\hat{F}_{(2+i)}}(\hat{E}^*_{2+i})) = \mathrm{Gal}(\hat{E}_{(2+i)}/\hat{F}_{(2+i)})$. By considering (7) we see that the elements $\{a, b, c\}$ are not norms. Because the elements $\{0, i, -1, -i, 1\}$ form a complete residue system of the group $\mathcal{O}_{\hat{E}_{(2+i)}}/(2+i)\mathcal{O}_{\hat{E}_{(2+i)}}$ we find that neither of the elements $\{i, -1\}$ is a norm.

The discriminant of the extension E/F has only two prime divisors $(2+i)$ and $(1+i)$ and therefore also the discriminant of the natural order of D_4 has only two prime divisors. This implies that the discriminant of the algebra is minimal.

TABLE II

$\mathbf{Q}(\omega)$-CENTRAL DIVISION ALGEBRAS WITH A UNIT γ

n	γ	f_n
2	$-\omega$	$x^2 + \sqrt{-3}$
3	ω	$x^3 - 2$
6	$-\omega^2$	$x^6 - 3\sqrt{-3}x^4 + 4x^3 - 9x^2 + 12\sqrt{-3}x + 3\sqrt{-3} + 4$

2) Center $\mathbf{Q}(\sqrt{-3})$*:* In Table II we give cyclic representations for algebras of degrees 2, 3, and 6. The theorem of Albert shows that 6 is the biggest degree we could hope to have a division algebra with a unit γ. We cannot have a division algebras of degrees 4 and 5 as tensoring these with a division algebra $\mathcal{G}_3$ (below) would respectively give us division algebras of degrees 12 and 15 with a unit γ.

We use the same generic notation as in the case of $\mathbf{Q}(i)$-central algebras.

Algebra $\mathcal{G}_2$*:* We use here the same methods that were used with the algebra $\mathcal{D}_4$. We remark that $(\sqrt{-3}) = P$ is tamely ramified in the extension E/F. If we pass to the completion E_P/F_P we get that the local conductor is P and that $\{-\omega, 1, 0\}$ is a complete set of representatives of the group $\mathcal{O}_{F_P/P}$. As a result it is seen that $-\omega$ is not a norm in the extension E_P/F_P and therefore it is not a norm in the extension E/F either. From this it follows that $\mathcal{G}_2$ is a division algebra.

By now it is obvious that the discriminant of the natural order of the algebra $\mathcal{G}_2$ has only two divisors $(\sqrt{-3})$, and (2) and hence the maximal order admits a minimal discriminant.

Algebra $\mathcal{G}_3$*:* The proof of this case is similar to that of $\mathcal{G}_2$ except that the tamely ramified prime P is 2 and that the suitable set of representatives is $\{1, \omega, \omega^2\}$.

Algebra $\mathcal{G}_6$*:* The algebra $\mathcal{G}_6$ we got as a tensor product from the algebras $\mathcal{G}_2$ and $\mathcal{G}_3$.

The postponed proof. When we were discussing the 6×6 perfect code we postponed the analysis of the algebra $\mathcal{B}_2 = (E/F, \sigma_2, -\omega)$, where $E/F = \mathbf{Q}(\sqrt{7}, j)/\mathbf{Q}(\omega)$. Now we have enough methods to attack this problem. We use similar strategy as in the case of the algebra $\mathcal{D}_4$.

The prime $(2 + \sqrt{-3}) = P_1$ is tamely ramified in the extension E/F. By passing to the P_1-adic completion $\hat{E}_{P_1}/\hat{F}_{P_1}$ we find that the local conductor is P_1. The image of the norm $N_{\hat{E}_{P_1}/\hat{F}_{P_1}}$ includes $\langle(1 + P_1)\rangle \times \langle e(2 + \sqrt{-3})\rangle$, where e is a unit of $\hat{F}_{P_1}$.

The set $\{0, 1, \omega, -\omega, \omega^2, -\omega^2\}$ is a complete residue system of the group $\mathcal{O}_{F_{P_1}}/P_1\mathcal{O}_{F_{P_1}}$ and whence

$$(F_{P_1})^* = \langle -j\rangle \times (1 + P_1) \times \langle e(2 + \sqrt{-3})\rangle.$$

On the other hand $\#((F_{P_1})^*/N_{E_{P_1}/F_{P_1}}(E^*_{P_1})) = 2$ and therefore $-j$ cannot be a norm. From this it follows that the local algebra $(\mathcal{B}_2)_{P_1}$ is a division algebra of index two.

There is no other choice for the Hasse invariant h_{P_1} than $1/2$.

Replacing the prime P_1 with $P_2 = (2 - \sqrt{-3})$ in previous considerations we see that $h_{P_2} = 1/2$.

The extension E/F has only three ramified primes $(2-\sqrt{-3})$, $(2+\sqrt{-3})$, and (2). Thus, the discriminant of the algebra $\mathcal{B}_2$ can have three prime divisors at maximum. The potential nontrivial Hasse invariants of $\mathcal{B}_2$ are now h_{P_1}, h_{P_2}, and $h_{(2)}$. The sum of h_{P_1} and h_{P_2} is 1 and therefore $h_{(2)}$ must be trivial.

B. General construction

In their recent paper [14] Elia et al. gave an explicit construction for division algebras of an arbitrary degree with centers $\mathbf{Q}(i)$ and $\mathbf{Q}(\sqrt{-3})$. In their general constructions they used non-unit, but relatively small γ's. As they were not interested in maximal orders nor the discriminants of the corresponding division algebras their algebras (with few exceptions) did not happen to have minimal discriminants.

We are now going to give a general construction for division algebras of arbitrary degree and with minimal discriminants. Due to Proposition 5.1 we can concentrate on algebras of prime power index. As a drawback our constructions will be dependent on the existence of certain prime numbers. We discuss this existence problem in Section VI-C which is purely number theoretic.

We first consider two easy prime powers and then move forward to more complicated ones.

For ease of notation in this subsection we will denote by $\mathbf{Z}_m$ the residue class ring modulo m, i.e. $\mathbf{Z}_m = \mathbf{Z}/m\mathbf{Z}$. Thus e.g. $\mathbf{Z}_m^*$ is logically the group of units of that ring.

Lemma 6.5: Suppose that E is a cyclic extension of F and that $a\mathcal{O}_E = P_1$ and P_2 are a pair of smallest primes in F. Assume that P_1 is totally inert and P_2 is the only ramified prime in the extension E/F. Then

$$\mathcal{A} = (E/F, \sigma, a),$$

where $\langle\sigma\rangle = \mathrm{Gal}(E/F)$, is a division algebra that has a minimal discriminant.

Proof: Lemma 6.4 combined with Proposition 2.1 gives that A is a division algebra. The minimality of the discriminant follows from Lemma 3.7. ■

Example 6.1: Lemma 6.5 is nothing but a simple generalization of Corollary 3.8 where we gave a construction for a family of $\mathbf{Q}(i)$-central division algebras of degree 2^k with a minimal discriminant.

Example 6.2: The field $\mathbf{Q}(\zeta_{3^{k+1}})$ has a unique subfield Z with $[Z : \mathbf{Q}] = 3^k$. The extension $\mathbf{Q}(\sqrt{-3})Z/\mathbf{Q}(\sqrt{-3})$ has degree 3^k and the prime (2) is totally inert in this extension. The extension also has a very limited ramification, the prime $(\sqrt{-3})$ is the only ramified one.

Primes $(\sqrt{-3})$ and (2) are a pair of minimal primes in the field $\mathbf{Q}(\sqrt{-3})$. Lemma 6.5 states now that the cyclic algebra $A = (\mathbf{Q}(\sqrt{-3})Z/\mathbf{Q}(\sqrt{-3}), \sigma, 2)$ is a division algebra with a minimal discriminant.

In Example 6.2 we found a suitable extension $E/\mathbf{Q}(\sqrt{-3})$ that only had one ramified prime $(\sqrt{-3})$. However we can prove that for an arbitrary degree there usually does not exist a cyclic extension that has ramification over $(\sqrt{-3})$ or (2) only. This assures that in general we cannot use such simple methods. Next we will provide a construction method that takes care of most of the prime power degrees. First we need some preliminary results.

We now present a global Frobenius automorphism. Suppose we have a finite Galois extension E/F and that B is such a prime ideal of $\mathcal{O}_E$ that $B \cap \mathcal{O}_F = P$ is unramified in the extension E/F. There exists a unique element $(B, E/F)$ of the group $\mathrm{Gal}(E/F)$ that is associated to the prime B. We call this element the Frobenius automorphism of B.

If the extension E/F is abelian, all the primes B_i that lie over P have the same Frobenius automorphism and we can denote $(B, E/F)$ by $(P, E/F)$.

For the definition and properties of the Frobenius automorphism we refer the reader to [31, p. 379].

We consider a tower of fields $F_1 \subseteq F_2 \subseteq E$ of finite extensions.

Proposition 6.6: If $F_1 \subseteq F_2 \subseteq E$, E/F_1 and F_2/F_1 are normal and B is such a prime ideal of E that $B \cap F_1 = P$ is unramified in E/F_1, then

$$(B, E/F_1)|_{F_2} = (B \cap F_2, F_2/F_1).$$

The prime P is totally inert in the extension E/F_1 if and only if $(B, E/F_1)$ generates the group $\mathrm{Gal}(E/F_1)$.

Proof: [31, Theorem 7.10, p. 380]. ■

The next lemma is a rather direct consequence of the definition of Hasse invariant.

Lemma 6.7: Let

$$\mathcal{A} = (E/F, \sigma, \gamma)$$

be a division algebra where $\langle \sigma \rangle = G(E/F)$, $\gamma \in F^*$, $[E : F] = n$ and suppose that P is a prime ideal of F that is totally inert in the extension E/F. If k is the smallest possible positive integer so that σ^k is the Frobenius automorphism of P then the Hasse invariant of P

$$h_P = \frac{k v_P(\gamma)}{n}.$$

Proof: [20, p. 281]. ■

Let us next consider a tower of fields $F_1 \subseteq F_2 \subseteq E$ of finite extensions and the proofs of the next two simple lemmas will be omitted.

Lemma 6.8: Let B be a prime ideal of E, $P_2 = \mathcal{O}_{F_2} \cap B$ and $P_1 = \mathcal{O}_{F_1} \cap B$.

1. Let $f(B/P_1)$, $f(B/P_2)$, and $f(P_2/P_1)$ be the respective inertia degrees of B over P_1, B over P_2, and P_2 over P_1. Then

$$f(B/P_1) = f(B/P_2) f(P_2/P_1).$$

2. Let $e(B/P_1)$, $e(B/P_2)$, and $e(P_2/P_1)$ be the respective ramification indices of B over P_1, B over P_2, and P_2 over P_1. Then

$$e(B/P_1) = e(B/P_2) e(P_2/P_1).$$

Lemma 6.9: Let E/F be a Galois extension, B a prime ideal of E and $P = F \cap B$. Then

$$e(B/P) \mid [E : F]$$

and

$$f(B/P) \mid [E : F].$$

Lemma 6.10: Let p be a prime and n such an integer that $n|(p-1)$. The field $\mathbf{Q}(\zeta_p)$ has a unique subfield Z with $[Z : \mathbf{Q}] = n$.

There exists a group isomorphism ϕ from $\mathbf{Z}_p^*/(\mathbf{Z}_p^*)^n$ to $\mathrm{Gal}(Z/\mathbf{Q})$ that takes any prime $p_i \neq p$ to the corresponding Frobenius automorphism $(p_1, Z/\mathbf{Q})$ in $\mathrm{Gal}(Z/\mathbf{Q})$.

The prime $p_1 \neq p$ is totally inert in the extension $Z/\mathbf{Q}$ if and only if p_1^t is not an nth power $\pmod p$ for $t = 1, \ldots, n-1$.

Proof: It is well known that there exists a unique isomorphism ψ from $\mathbf{Z}_p^*$ to $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ which takes prime $p_1 \neq p$ to $(p_1, \mathbf{Q}(\zeta_p)/\mathbf{Q})$. We denote the fixed field of the group $\psi(\mathbf{Z}_p^*)^n$ by Z. It is now clear that Z is unique and $[Z : \mathbf{Q}] = n$. If we first map the elements of $\mathbf{Z}_p^*$ with ψ to $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ and then restrict the resulting automorphisms to the field Z, we obtain an isomorphism ϕ from $\hat{\mathbf{Z}}_p^*/(\hat{\mathbf{Z}}_p^*)^n$ to $\mathrm{Gal}(Z/\mathbf{Q})$. Proposition 6.6 states that ϕ has the claimed properties.

The last claim follows from the properties of ϕ combined with the last statement of Proposition 6.6. ■

Proposition 6.11: Suppose that $F = \mathbf{Q}(\sqrt{c})$ is a quadratic field, $q \neq 2$ is a given prime and n a given integer. We suppose that P_1 and P_2 are the smallest primes ideals in F and p_1 and p_2 are the prime numbers that lie under P_1 and P_2.

Let p be such a prime that $q^n|(p-1)$, $(p, c) = 1$ and that p_1 and p_2 are totally inert in the extension $Z/\mathbf{Q}$, where Z is the unique subfield of $\mathbf{Q}(\zeta_p)$ of degree q^n. We also suppose that p is inert in the extension $F/\mathbf{Q}$.

The extension FZ/F is a cyclic Galois extension of degree q^n where the prime ideals P_1 and P_2 are totally inert and $P = p\mathcal{O}_F$ is the only ramified prime ideal in the extension FZ/F.

Proof: Let B be a prime ideal of FZ, $P_Z = \mathcal{O}_Z \cap B$, $P_F = \mathcal{O}_F \cap B$ and $b = \mathbf{Q} \cap B$. We denote the corresponding ramification indices by $e(B/P_Z)$, $e(P_Z/P_F)$ and $e(P_F/b)$. According to Lemma 6.8

$$e(B/b) = e(B/P_Z)e(P_Z/b) = e(B/P_F)e(P_F/b).$$

Lemma 6.9 for its part states that $e(B/P_Z), e(P_F/b) \mid 2$ and $e(P_Z/b), e(B/P_F) \mid q^n$. This together with the previous equation shows that the prime $P_F \subset \mathcal{O}_F$ is ramified in the extension FZ/F if and only if the prime b is ramified in the extension $Z/\mathbf{Q}$.

The prime p is the only ramified prime in $Z/\mathbf{Q}$ and because p is inert in the extension $F/\mathbf{Q}$ we see that P is the only ramified ideal in the extension ZF/F.

If we choose B so that $P_F = P_1$ or $P_F = P_2$, then

$$f(B/b) = f(B/P_Z)f(P_Z/b) = f(B/P_F)f(P_F/b) = q^n \cdot c,$$

where $c = 1$ or $c = 2$. This combined with Lemma 6.9 implies that $f(B/P_F) = q^n$. ■

In the following propositions we use the notation from Proposition 6.11.

Proposition 6.12: There exists such a group isomorphism between $\mathrm{Gal}(FZ/F)$ and $\mathrm{Gal}(Z/\mathbf{Q})$ that every Frobenius automorphism of $B \subset \mathcal{O}_{FZ}$ maps to the Frobenius automorphism of $B \cap Z = B_Z$.

Proof: It is a well-known fact that there exists a well defined surjective homomorphism from $\mathrm{Gal}(FZ/\mathbf{Q})$ to $\mathrm{Gal}(Z/\mathbf{Q})$ for which $\sigma \longmapsto \sigma|_Z$. The kernel of this map consists of those elements of $\mathrm{Gal}(FZ/\mathbf{Q})$ that act trivially on the field Z. On the other hand, if we restrict the domain of the map to those elements that act trivially on F this map is an injection because the only element of $\mathrm{Gal}(FZ/\mathbf{Q})$ that acts trivially on both fields F and Z is the identity map. As we know that $|\mathrm{Gal}(FZ/F)| = |\mathrm{Gal}(Z/\mathbf{Q})|$ the described map must be an isomorphism. Now the statement about Frobenius maps follows from Proposition 6.6. ■

Proposition 6.13: Let

$$p_2 p_1 = 1 \tag{8}$$

in the group $\mathbf{Z}_p^*/(\mathbf{Z}_p^*)^{q^n}$, $P_1 = a_1\mathcal{O}_F$, and $P_2 = a_2\mathcal{O}_F$. Then

$$\mathcal{A} = (FZ/F, \sigma, a_1 a_2)$$

with $\langle\sigma\rangle = \mathrm{Gal}(FZ/F)$ is a division algebra that has a minimal discriminant.

Proof: The prime P_1 is totally inert in the extension FZ/F. Thus, Lemma 6.4 states that $\mathcal{A}$ is a division algebra.

From the cyclic presentation of the algebra $\mathcal{A}$ we instantly see that $\mathcal{A}$ has only three Hasse invariants that can be nontrivial: h_{P_1}, h_{P_2}, and h_P. In what follows we are going to show that the invariant h_P must be trivial.

We first choose σ to be the Frobenius automorphism of P_1. Lemma 6.7 now shows that the Hasse invariant of P_1 is

$$\frac{1}{q^n} = h_{P_1}.$$

Because the group $\mathbf{Z}_p^*/(\mathbf{Z}_p^*)^{q^n}$ is cyclic we get from (8) that $p_2 = p_1^{q^n-1}$ in $\mathbf{Z}_p^*/(\mathbf{Z}_p^*)^{q^n}$. This implies that $(P_2, FZ/F) = \sigma^{n-1}$. Lemma 6.7 then states that

$$\frac{q^n-1}{q^n} = h_{P_2}.$$

The sum of the Hasse invariants of $\mathcal{A}$ must be zero $\pmod 1$, whence

$$h_{P_1} + h_{P_2} + h_P \in \mathbf{Z}.$$

But, we already saw that $h_{P_1} + h_{P_2} \in \mathbf{Z}$, which implies that $h_P \in \mathbf{Z}$. The discriminant of the algebra $\mathcal{A}$ has now only two divisors P_1 and P_2.

In the beginning of our proof we make the assumption that σ is the Frobenius of the prime P_1. However, the choice of the generator of the group $\mathrm{Gal}(FZ/F)$ in a cyclic representation does not change the discriminant of the corresponding algebra. ■

Example 6.3: Suppose that the center $F = \mathbf{Q}(i)$. The primes $(1+i)$ and $(2+i)$ are a pair of smallest prime ideals in this field. We want to produce a division algebra of index 10 that has a minimal discriminant. It is not difficult to check that 2^t and 5^t are not 5th powers $\pmod{11}$ for $t = 1, \ldots, 4$, and that 11 is inert in the extension $F/\mathbf{Q}$. Lemma 6.11 states that $\mathbf{Q}(\zeta_{11})$ has a subfield Z, $[Z : \mathbf{Q}] = 5$, and that 2 and 5 are totally inert in the extension $Z/\mathbf{Q}$.

Proposition 6.11 states that the primes $(1+i)$ and $(2+i)$ are totally inert in the extension FZ/F and the prime ideal $11\mathcal{O}_F$ is the only ramified ideal in the extension FZ/F.

We easily see that $2 \cdot 5 = 1$ in $\mathbf{Z}_{11}^*/(\mathbf{Z}_{11}^*)^5$. Therefore,

$$(FZ/F, \sigma_1, (1+i)(2+i))$$

is a division algebra with a minimal discriminant.

We previously saw that $\mathcal{A} = (\mathbf{Q}(\zeta_{2^4})/F, \sigma_2, 2+i)$ is a division algebra of index 2 and has a minimal discriminant. Finally, from Proposition 5.1

$$(\mathbf{Q}(\zeta_{2^4})Z/F, \sigma_1\sigma_2, (1+i)^2(2+i)^7)$$

is seen to be a division algebra of degree 10 with a minimal discriminant.

C. Existence of suitable primes

Propositions 6.11 and 6.13 have turned our construction project into a hunt of suitable prime numbers. The problem is that we do not know if there are "enough" suitable prime numbers. The answer is that in most cases there are. This will be proved in Theorem 6.17, but first we need some preliminary results.

For the definition and the basic properties of Kummer extensions we refer the reader to [29, p. 197].

Proposition 6.14: Let E/F be a Kummer extension with $E = F(\alpha)$, $\alpha^n = a \in \mathcal{O}_F$, and let P be a prime ideal of F that is not a divisor of $a \cdot n$. Furthermore, let t be the largest divisor of n such that the congruence

$$x^t \equiv a \pmod{p}$$

has a solution in $\mathcal{O}_F$. Then P decomposes in E into a product of t prime ideals of degree n/t over P.

Proof: [29, Theorem 6.8.4, p. 197]. ■

Lemma 6.15: Suppose that q and p are prime numbers and that $q^t|(p-1)$ for some integer t. If c is an integer and the equation

$$c \equiv x^q \pmod{p} \tag{9}$$

is not solvable, then neither is any of the equations

$$c^k \equiv x^{q^t} \pmod{p}, \tag{10}$$

where $k = 1, \ldots, q^t - 1$.

Proof: Let a be a generator of the cyclic group $\mathbf{Z}_p^*$. Then we can write that $c \equiv a^n \pmod{p}$ for some integer n.

Let us assume that (9) has no solution. This implies that q is not a factor of n. Assume then that for some k there is a solution d for (10). If we write $d \equiv a^s$, then (10) gives that $kn - sq^t = v(p-1)$, where v is some integer. As $q^t|(p-1)$ this would mean that $q^t|kn$. That gives us a contradiction. ■

In the following we use the phrase "the prime P has inertia in the extension E/F". By that we mean that at least one prime ideal B of E that lies over the P has inertial degree $f(P|B) > 1$.

Lemma 6.16: Suppose that F_1 and F_2 are Galois extensions of a field F and $F_1 \cap F_2 = F$. The prime P of $\mathcal{O}_F$ has inertia in the extension F_1F_2 if and only if it has inertia in the extension F_1 or F_2. The prime P is ramified in the extension F_1F_2 if and only if it is ramified in F_1 or in F_2.

Proof: For the proof the reader is referred to [32, p. 263]. ■

The proof of the following theorem is a slightly modified version of the proof of [33, Theorem 1]. We do not suppose here that the center is totally complex nor that the ring $\mathcal{O}_F$ is a PID. However, we suppose that $p_1 \neq p_2$.

Theorem 6.17: Assume that $F = \mathbf{Q}(\sqrt{c})$ is a quadratic field, P_1 and P_2 are the smallest primes in F, $q \neq 2$ is a given prime, and n a given integer. Let us also suppose that p_1 and p_2 are prime numbers that lie under P_1 and P_2.

If $q \nmid c$, then there exists infinitely many prime numbers p so that p is inert in F, $\mathbf{Q}(\zeta_p)$ has a unique subfield Z, $[Z : \mathbf{Q}] = q^n$, where p_1 and p_2 are totally inert, and $p_1p_2 = 1$ in $\mathbf{Z}_p^*/(\mathbf{Z}_p^*)^{q^n}$.

Proof: Let us denote $q^n = s$, $\mathbf{Q}(\zeta_s)((p_1p_2)^{1/s}) = K$, $K((p_1)^{1/q}) = K_1$ and suppose that $q \neq p_1$. By considering the prime ideal factorization of p_1p_2 in $\mathbf{Q}(\zeta_s)$ we may conclude that $(p_1p_2)^d$ cannot be an sth power for any $d = 1, \ldots, s-1$. Therefore $[K : \mathbf{Q}(\zeta_s)] = s$.

As we have supposed that $q \nmid c$ there has to be at least one prime p_3 that has a ramification index 2 in the extension $F/\mathbf{Q}$, but is not ramified in the extension $\mathbf{Q}(\zeta_s)/\mathbf{Q}$. Earlier, we saw that $[K : \mathbf{Q}(\zeta_s)] = s$. Because p_3 is not ramified in $F/\mathbf{Q}$ and 2 does not divide $[K : \mathbf{Q}(\zeta_s)]$, none of the prime ideals P_3 in $\mathcal{O}_K$ that lies over p_3 has 2 as a divisor of the ramification index $e(P_3|p_3)$. This implies that $F \nsubseteq K$.

By [33, Lemma 2] we know that $[K_1 : K] = q$. Because $q \neq 2$ and $F \nsubseteq K$ the extension K_1F/K is cyclic and $[K_1F : K] = 2q$.

Chebotarev's density theorem [31, Lemma 7.14, p. 392] states that K has infinitely many prime ideals that have absolute degree one and are totally inert in the extension $K(\sqrt[q]{p_1})F/K$. We choose one, P, that not only has an absolute degree one but that is also unramified in the extension $K/\mathbf{Q}$.

We denote the prime of $\mathbf{Q}$ that lies under P by p. The field $\mathbf{Q}(\zeta_{q^n})$ is a subfield of K and therefore p splits completely in the extension $\mathbf{Q}(\zeta_{q^n})/\mathbf{Q}$. The theory of cyclotomic fields [29, p. 195] now gives that

$$p \equiv 1 \pmod{q^n}.$$

Next we are going to show that p_1^t is not an sth power $\pmod{p}$ for $t = 0, \ldots, s-1$. We assume the contrary. Suppose that $p_1 \equiv a^q \pmod{p}$ for some integer a. Now $p_1 \equiv a^q \pmod{P}$. This last equation however cannot be true because P is totally inert in the Kummer extension K_1/K. Lemma 6.15 now states that equation $p_1 \equiv x^t \pmod{p}$ does not have a solution for any $t = 1, \ldots, q^n - 1$.

Lemma 6.10 states that $\mathbf{Q}(\zeta_p)$ has a unique subfield Z with $[Z : \mathbf{Q}] = q^n$, and that p_1 is totally inert in the extension $Z/\mathbf{Q}$.

The prime P has absolute degree one in K and therefore $(p_1p_2)^{1/q^n} \equiv c \pmod{P}$, where c is some integer. This implies that

$$p_1p_2 \equiv c^{q^n} \pmod{p}.$$

If we use the notation of Lemma 6.10, the map ϕ takes p_1 to the generator g of the group $\mathrm{Gal}(Z/\mathbf{Q})$ and $p_1 \cdot p_2$ to identity. The map ϕ is a homomorphism and therefore $\phi(p_2) = g^{-1}$, which again is a generator of the group $\mathrm{Gal}(Z/\mathbf{Q})$. Lemma 6.10 now shows that p_2 is totally inert in the extension $Z/\mathbf{Q}$.

To complete the proof we have to show that the prime p is inert in the extension $F/\mathbf{Q}$. The prime P must be inert in the extension FK/K and therefore the prime p has at least some inertia in the extension $FK/\mathbf{Q}$. Because p is totally split in the extension $K/\mathbf{Q}$ it does not have any inertia in this extension and therefore Lemma 6.16 states that p must be inert in the extension $F/\mathbf{Q}$. ■

Theorem 6.17 states that for the center $\mathbf{Q}(i)$ the only problematic prime power indices are of the form 2^k. Luckily, the construction of Corollary 3.8 covers these cases. As a consequence, we can construct a division algebra with a minimal discriminant for an arbitrary index. In Table III we give explicit representations for division algebras with a prime power index (< 20) and a minimal discriminant.

For each index q^n we have searched the prime p of the Theorem 6.17 along the lines of Example 6.3. After the prime p is found the actual minimal polynomial of the extension $FZ/F\mathbf{Q}$ can be easily found by considering the subfields of the extension $\mathbf{Q}(\zeta_p)/\mathbf{Q}$. Both tasks were done with the aid of computer algebra system PARI [34].

If the center is $\mathbf{Q}(\sqrt{-3})$, the problematic prime powers are 2^n and 3^n. Algebras of degree 3^n we get from Example 6.2, but degrees 2^n are more problematic. Still for indices 2 and 4 we can find suitable primes even when Theorem 6.17 is not promising anything. As a conclusion we can construct a division algebra with a minimal discriminant if the index is not divisible by 8.

In Table IV we give explicit representations for our algebras.

Example 6.4: From Table III we get that

$$\mathcal{A}_3 = (\mathbf{Q}(i)(a_3)/\mathbf{Q}(i), \sigma_3, (1+i)(2+i))$$

and

$$\mathcal{A}_2 = (\mathbf{Q}(i)(a_2)/\mathbf{Q}(i), \sigma_2, (2+i))$$

are division algebras with minimal discriminants. According to Proposition 5.1 algebra $\mathcal{A}_2 \otimes \mathcal{A}_3 = (\mathbf{Q}(i)(a_6)/\mathbf{Q}(i), \sigma_2\sigma_3, (2+i)^5(1+i)^2)$, where a_6 is a zero of the polynomial $x^6 - 2x^5 + (-3i-51)x^4 + (4i-30)x^3 + (-2i+755)x^2 + (-298i+2134)x + -593i + 1628$, is a division algebra of degree 6 and has a minimal discriminant.

One of the unfortunate properties of our construction is that when we produce division algebras of a composite index the resulting algebras tend to have relatively large non-norm elements γ. In the following example we solve this problem in one specific case and show that we can always use $\gamma = (2+i)(1+i)$. The method has a straightforward generalization to more common situations.

Example 6.5: In what follows we produce the algebra $\mathcal{A}_6$ as a tensor product of two smaller algebras.

Let a_2 be a zero of the polynomial $x^2 + i$. The algebra $\mathcal{B}_2 = (F(a_2)/F, \sigma_2, (1+i)(2+i))$ is a slightly modified version of the algebra $\mathcal{A}_2$ of Table III. It is a division algebra with a minimal discriminant.

The algebra $\mathcal{B}_3 = (F(a_3)/F, \sigma_3, (2+i)^{-1}(1+i)^{-1})$ is a modified version of the algebra $\mathcal{A}_3$. Proposition 6.4 gives us that $\mathcal{B}_3$ is still a division algebra. By considering the equation $\mathcal{B}_3 \otimes \mathcal{A}_3 \sim M_n(F)$ we see that $\mathcal{B}_3$ has the same discriminant as the algebra $\mathcal{A}_3$.

Because $\mathcal{B}_2$ and $\mathcal{B}_3$ are division algebras with minimal discriminants it follows from Proposition 5.1 that the tensor product $\mathcal{A}_6 = \mathcal{B}_3 \otimes \mathcal{B}_2 = (F(b_2, a_3)/F, \sigma_2\sigma_3, (2+i)(1+i))$ is a division algebra with a minimal discriminant. The polynomial f_6 is just simply the minimal polynomial of the generator a_6 of the field $F(b_2, a_3)$.

VII. An example code and some simulation results

One of the ingredients in the construction of the perfect codes was the use of ideals in improving the shape of the code lattices. In [5] we did the same but for the purpose of saving energy and making the lattice easier to encode. We include the following simple fact (also known to E. Viterbo, private communication) explaining why using a principal one-sided (left or right) ideal instead of the entire order will not change the density of the code.

Lemma 7.1: Let Λ be a maximal order in a cyclic division algebra of index n over an imaginary quadratic number field. Assume that the minimum determinant of the lattice Λ is equal to one. Let $x \in \Lambda$ be any non-zero element. Let $\rho > 0$ be a real parameter chosen such that the minimum determinant of the lattice $\rho(x\Lambda)$ is also equal to one. Then the fundamental parallelotopes of these two lattice have the same measure

$$m(\Lambda) = m(\rho(x\Lambda)).$$

Proof: By multiplicativity of the norm the minimum determinant of $x\Lambda$ is equal to the absolute value of $nr(x)$, so the parameter ρ is the unique positive root of the equation

$$\rho^n |nr(x)| = 1.$$

TABLE III

CONDUCTOR p OF THE CYCLOTOMIC FIELD $\mathbf{Q}(\zeta_p)$, γ, AND THE MINIMAL POLYNOMIAL f_n OF THE EXTENSION $\mathbf{Q}(i)(a_n)/\mathbf{Q}(i)$

n	p	γ	f_n
2		$(2+i)$	x^2+i
3	79	$(1+i)(2+i)$	$x^3+x^2-26x+41$
4		$(2+i)$	x^4+i
5	11	$(1+i)(2+i)$	$x^5+x^4-4x^3-3x^2+3x+1$
7	211	$(1+i)(2+i)$	$x^7+x^6-90x^5+69x^4+1306x^3+124x^2-5249x-4663$
8		$(2+i)$	x^8+i
9	271	$(1+i)(2+i)$	$x^9+x^8-120x^7-543x^6+858x^5+6780x^4+7217x^3-2818x^2-4068x-261$
11	859	$(1+i)(2+i)$	$x^{11}+x^{10}-390x^9-653x^8+52046x^7+146438x^6-2723930x^5-11558015x^4+36326009x^3+250960565x^2+385923388x+145865807$
13	6163	$(1+i)(2+i)$	$x^{13}+x^{12}-2844x^{11}-6017x^{10}+2908490x^9+10238862x^8-1340405033x^7-6785664624x^6+281925130086x^5+1909036915713x^4-21097272693753x^3-192054635052100x^2-235667966495418x+213548387827457$
16		$(2+i)$	$x^{16}+i$
17	239	$(1+i)(2+i)$	$x^{17}+x^{16}-112x^{15}-47x^{14}+3976x^{13}+4314x^{12}-64388x^{11}-136247x^{10}+422013x^9+1631073x^8+411840x^7-5840196x^6-11894369x^5-10635750x^4-4739804x^3-938485x^2-54850x-619$
19	8779	$(1+i)(2+i)$	$x^{19}+x^{18}-4158x^{17}+8463x^{16}+6281539x^{15}-34466097x^{14}-4291513699x^{13}+39454551948x^{12}+1357034568541x^{11}-17014625218525x^{10}-184614267432185x^9+3035523756071878x^8+10088401800577582x^7-253111326110358151x^6-1432084484613198668x^5+10612439791376560471x^4-37745592327983578892x^3-22004164792391296318 2x^2+86083932120501598139x+179422120229746149964 1$

Let us denote this by

$$\rho = |\frac{1}{nr(x)}|^{1/n}.$$

On the other hand, the index $[\Lambda : x\Lambda] = |N_{\mathcal{A}/\mathbf{Q}}(x)|$ (see [20, Exercise 7, p. 131]). Moreover, [20, Theorem 9.14, p. 119] tells us that

$$|N_{\mathcal{A}/\mathbf{Q}}(x)| = |N_{F/\mathbf{Q}}(N_{\mathcal{A}/F}(x))| \overset{\textbf{Remark 2.1}}{=} |N_{F/\mathbf{Q}}(nr(x)^n)| \overset{[F:\mathbf{Q}]=2}{=} |nr(x)^n|^2 = |nr(x)|^{2n}.$$

Hence, $[\Lambda : x\Lambda] = |nr(x)|^{2n}$. Scaling the lattice $x\Lambda$ by the factor ρ will multiply the measure of the fundamental parallelotope by ρ^{2n^2}. The claim immediately follows from these facts by calculating

$$m(\rho(x\Lambda)) = \rho^{2n^2} m(x\Lambda) = |\frac{1}{nr(x)}|^{2n^2/n}\ [\Lambda : x\Lambda]\ m(\Lambda) = |\frac{1}{nr(x)}|^{2n}\ |nr(x)|^{2n}\ m(\Lambda) = m(\Lambda).$$

■

We remark that the same fact obviously also holds for principal left ideals of a maximal order. A way of using the above lemma is that we can choose the element x in such way that the left (or right) ideal $x\Lambda$ is contained in the natural order. By moving the code inside the natural order we then to some extent recover the layered structure of the natural orders, and then, hopefully, also some of the advantages of the inherent orthogonality between layers.

TABLE IV

CONDUCTOR p OF THE CYCLOTOMIC FIELD $\mathbf{Q}(\zeta_p)$, γ, AND THE MINIMAL POLYNOMIAL f_n OF THE EXTENSION $\mathbf{Q}(\sqrt{-3})(a_n)/\mathbf{Q}(\sqrt{-3})$

n	p	γ	f_n
2	5	$(\sqrt{-3})(2)$	x^2+x-1
3		(2)	x^3-3x+1
4	5	$(\sqrt{-3})(2)$	$x^4+x^3+x^2+x+1$
5	101	$(\sqrt{-3})(2)$	$x^5+x^4-40x^3+93x^2-21x-17$
7	197	$(\sqrt{-3})(2)$	$x^7+x^6-84x^5-217x^4+1348x^3+3988x^2-1433x-1163$
8			
9		(2)	$x^9-9x^7+27x^5-30x^3+9x+1$
11	353	$(\sqrt{-3})(2)$	$x^{11}+x^{10}-160x^9-525x^8+6066x^7+26034x^6-48369x^5-265374x^4-42966x^3+405001x^2+63189x-170569$
13	4889	$(\sqrt{-3})(2)$	$x^{13}+x^{12}-2256x^{11}+15535x^{10}+1555245x^9-20301911x^8-255557592x^7+4688166666x^6+3148489502x^5-327998691680x^4+1203189132463x^3+3781862679467x^2-26224493395483x+33207907136809$
16			
17	9011	$(\sqrt{-3})(2)$	$x^{17}+x^{16}-4240x^{15}+17305x^{14}+5727403x^{13}-41284287x^{12}-2705219919x^{11}+14589308035x^{10}+564280956214x^9-1381250312443x^8-51961946136288x^7+526852031838x^6+1834916754576839x^5+1836850197549204x^4-23335163152861586x^3-34406356236297728x^2+60102147038980885x+73569709231092527$
19	8171	$(\sqrt{-3})(2)$	$x^{19}+x^{18}-3870x^{17}+41421x^{16}+3724805x^{15}-43503449x^{14}-1437461514x^{13}+12225751511x^{12}+286728047867x^{11}-968096767438x^{10}-28322179217822x^9-31203374649750x^8+994413740064487x^7+3501119135247182x^6-8098862899035075x^5-59620882192114428x^4-90513387045636018x^3-3449524754137218x^2+73725797301678129x+35046894150872059$

For example in the case of the Golden+ algebra we can use the element $(1-\lambda)^3$ from the ring of integers $\mathcal{O}_E$ of the larger field $E=\mathbf{Q}(\sqrt{2+i})$ as a multiplier. Thus, by denoting

$$M=\begin{pmatrix}(1-\lambda)^3 & 0\\ 0 & (1+\lambda)^3\end{pmatrix}$$

we get the ideal $\mathcal{I}$ consisting of matrices of the form $aMM_1+bMM_2+cMM_3+dMM_4$, where the coefficients a,b,c,d are Gaussian integers and the matrices $M_j, j=1,2,3,4$ are from Section IV-A. This ideal is a subset of the natural order $\mathcal{O}_E\oplus u\mathcal{O}_E$.

Our code constructions are based on selecting the prescribed number of lowest energy matrices from a chosen additive coset of the ideal $\mathcal{I}$. In order to reach a target bandwidth utilization of 4, 5 or 6 bpcu we thus selected 256, 1024 or 4096 matrices. In this sense we have done some coset optimization for the Golden+ codes, but make no claims as to having found the best coset. For the rival Golden code from [10] the coset corresponding to assigning all the Gaussian integers the value $(1+i)/2$ stands out. This is because then there are 256 matrices all having the minimal energy, and more importantly because in that case pulse amplitude modulation (PAM) can be used to good effect. We first did some simulations using a PAM-type rule for larger subsets of the Golden code as well by arbitrarily selecting a suitable number of coefficients of the basis matrices from the set $\{-3/2,-1/2,1/2,3/2\}$ so that the desired bandwidth efficiency was achieved. This is a natural choice well suited for e.g. the sphere decoding algorithm. While we ended up having a dead even race BLER-wise at 4.0 bpcu, the Golden code lost to the Golden+ code by about 0.9 dB at the higher rates (see Figure 1). In the interest of a fair comparison we then tried

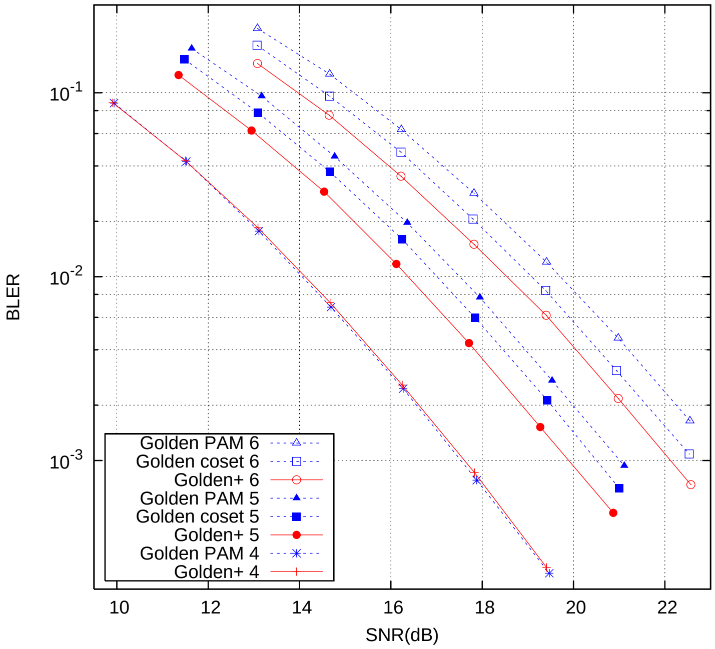

Fig. 1. Block error rates at 4, 5, and 6 bpcu.

coset optimization for the Golden code as well. This narrowed down the gap to about 0.3 dB. However, the resulting subsets of the Golden code no longer have such a structure well suited to PAM. In other words both the rival codes must resort to the use of a code book. We have not even attempted to solve the problem of optimizing the code book for the purposes of minimizing BER. This also explains, why our performance plots only show the block error rates (i.e. the probability of decoder deciding in favor of a 2×2 matrix other than the transmitted one) rather than bit error rates. Thus, our simulations may also be viewed as measuring the amount of power lost, when one insists on not needing a code book.

VIII. Concluding remarks and suggestions for further work

We have derived a bound for the density of fully multiplexing MIMO matrix lattices resulting in codes with a unit minimum determinant. The bound only applies to codes gotten from the cyclic division algebras and their ideals. While the bound is not constructive per se, we also showed that it can be achieved for any number of transmit antennas, and discussed techniques leading to the construction of CDAs with maximal orders attaining the bound. R. Vehkalahti is preparing an even more number theoretical article, where these techniques are expanded. We also discussed the Ivanyos–Rónyai algorithm that is needed to actually find these densest possible lattices inside these CDAs, and gave as an example a construction of a fully multiplexing 2×2 code that outperforms the Golden code at least for some data rates.

We have not yet exhausted the box of optimization tools on our code. E.g. the codes can be pre- and postmultiplied by any complex matrix of determinant one without affecting neither its density nor its good minimum product distance. In particular, if we use non-unitary matrix multipliers, the geometry of the lattice will change. While we cannot turn the lattice into a rectangular one in this manner, some energy savings and perhaps also shaping gains are available, but we have not solved the resulting optimization problem yet. Hopefully a suitably reformed version of our lattice will also allow a relatively easy description of the low energy matrices. This in turn would make the use of the sphere decoding algorithm on our lattice more attractive.

There are also possibilities for applying these class field theoretical techniques to slightly modified density problems of ST-codes. E.g. it is probably relatively easy to adapt the bound of Theorem 3.2 to the case of multi-block ST-codes. Another possibility is to study the cases, where the codes are not fully multiplexing. Such situations arise naturally in an application, where the receiver may have a lower number of antennas, e.g. in a cellular phone downlink.

An immediate open problem is to utilize maximal orders of the cyclic division algebra of index 2 with center $\mathbf{Q}(\omega)$. When looking for the example code in the previous section a natural step was to use LLL-algorithm for finding a relatively orthogonal basis for the lattice. That definitely aided the search for a good coset. In the hexagonal case this step is somewhat trickier and using a multiplier to put the maximal order inside the natural order only lead to a code with a disappointing performance. The best way of using this densest known lattice of 2×2-matrices is not known to us. As another open problem we ask, whether the discriminant bound can be broken by a MIMO lattice that does not come from a cyclic division algebra. We believe this to be a very difficult question.

IX. Acknowledgments

We are grateful to professor Lajos Rónyai for explaining to us many details of his algorithm for finding maximal orders.

References

[1] J.-C. Guey, M. P. Fitz, M. R. Bell, and W. Y. Kuo, “Signal design for transmitter diversity wireless communication systems over Rayleigh fading channels”, in *Proc. IEEE Vehicular Technology Conf.*, 1996, pp. 136–140. Also in *IEEE Trans. Commun.*, vol. 47, pp. 527–537, April 1999.

[2] V. Tarokh, N. Seshadri, and A.R. Calderbank, “Space-Time Codes for High Data Rate Wireless Communications: Performance Criterion and Code Construction”, *IEEE Transactions on Information Theory*, vol. 44, pp. 744–765, March 1998.

[3] J.-C. Belfiore, G. Rekaya, and E. Viterbo: “The Golden Code: A 2x2 Full-Rate Space-Time Code With Non-vanishing Determinant”, *IEEE Transactions on Information Theory*, vol. 51, n. 4, pp. 1432–1436, April 2005.

[4] S. M. Alamouti, “A Simple Transmit Diversity Technique for Wireless Communication”, *IEEE J. on Select. Areas in Commun.*, vol. 16, pp. 1451–1458, October 1998.

[5] C. Hollanti and J. Lahtonen, “Maximal Orders in the Design of Dense Space-Time Lattice Codes”, submitted to *IEEE Transactions on Information Theory*, September 2006.

[6] M. O. Damen, K. Abed-Meraim, and J.-C. Belfiore, “Diagonal Algebraic Space-Time Block Codes”, *IEEE Trans. Inf. Theory*, vol. 48, pp. 628–636, March 2002.

[7] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, “Full-Diversity, High-Rate Space-Time Block Codes From Division Algebras”, *IEEE Trans. Inf. Theory*, vol. 49, pp. 2596–2616, October 2003.

[8] J.-C. Belfiore and G. Rekaya, “Quaternionic Lattices for Space-Time Coding”, in *Proc. ITW 2003*, Paris, France, March 31 - April 4, 2003.

[9] J.-C. Belfiore, G. Rekaya, and E. Viterbo, “Algebraic 3x3, 4x4 and 6x6 Space-Time Codes with Non-Vanishing Determinants”, in *Proc. IEEE ISITA 2004*, Parma, Italy, October 10 - 13, 2004.

[10] J.-C. Belfiore, F. Oggier, G. Rekaya, and E. Viterbo, “Perfect Space-Time Block Codes”, *IEEE Trans. Inf. Theory*, vol. 52, pp. 3885–3902, September 2006.

[11] Kiran. T and B. S. Rajan, “STBC-Schemes with Non-Vanishing Determinant For Certain Number of Transmit Antennas”, *IEEE Trans. Inf. Theory*, vol. 51, pp. 2984–2992, August 2005.

[12] V. Shashidhar, B. S. Rajan, and B. A. Sethuraman “STBCs using capacity achieving designs from crossed-product division algebras”, in *Proc. IEEE ICC 2004*, pp. 827–831, Paris, France, 20-24 June 2004.

[13] V. Shashidhar, B. S. Rajan, and B. A. Sethuraman, “Information-Lossless STBCs from Crossed-Product Algebras”, *IEEE Trans. Inf. Theory*, vol. 52, pp. 3913–3935, September 2006.

[14] P. Elia, K. R. Kumar, P. V. Kumar, H.-F. Lu, and S. A. Pawar, “Explicit Space-Time Codes Achieving the Diversity-Multiplexing Gain Tradeoff”, *IEEE Trans. Inf. Theory*, vol. 52, pp. 3869–3884, September 2006.

[15] G. Wang and X.-G. Xia, “On Optimal Multi-Layer Cyclotomic Space-Time Code Designs”, *IEEE Trans. Inf. Theory*, vol. 51, pp. 1102–1135, March 2005.

[16] L. Zheng and D. Tse, “Diversity and Multiplexing: A Fundamental Tradeoff in Multiple-Antenna Channels”, *IEEE Trans. Inf. Theory*, vol. 49, pp. 1073–1096, May 2003.

[17] H. El Gamal and A. R. Hammons, Jr., “A new approach to layered space-time coding and signal processing,” *IEEE Trans. Inf. Theory*,vol. 47, pp. 2321–2334, Sep. 2001.

[18] G. Ivanyos and L. Rónyai, “On the complexity of finding maximal orders in algebras over Q”, Computational Complexity 3, pp. 245–261, 1993.

[19] Web page: http://magma.maths.usyd.edu.au/magma/htmlhelp/text835.htm#8121.

[20] I. Reiner, *Maximal Orders*, Academic Press, New York 1975.

[21] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo, “Algebraic Lattice Constellations: Bounds on Performance”, *IEEE Transactions on Information Theory*, vol. 52, n. 1, pp. 319–327, January 2006.

[22] N. Jacobson, *Basic Algebra II*, W. H. Freeman and Company, San Francisco 1980.

[23] A. A. Albert, *Structure of Algebras*, American Mathematical Society, New York City 1939.

[24] J. S. Milne , *Class Field Theory*, Lecture notes for a course given at the University of Michigan, Ann Arbor, http://www.jmilne.org/math/coursenotes/.

[25] C. Hollanti and J. Lahtonen, “A New Tool: Constructing STBCs from Maximal Orders in Central Simple Algebras”, in *Proc. IEEE ITW 2006*, pp. 322–326, Punta del Este, March 13-17, 2006.

[26] L. Rónyai, “Algorithmic Properties of Maximal Orders in Simple Algebras Over Q”, *Computational Complexity 2*, pp. 225–243, 1992.

[27] C. Hollanti, J. Lahtonen, K. Ranto, and R. Vehkalahti, “Optimal Matrix Lattices for MIMO Codes from Division Algebras”, in *Proc. IEEE ISIT 2006*, pp. 783–787, Seattle, July 9 - 14, 2006.

[28] L. Rónyai, “Computing the Structure of Finite Algebras”, *Journal of Symbolic Computation 9*, pp. 355–373, 1990.

[29] H. Koch, *Number Theory, Algebraic Numbers and Functions*. American Mathematical Society, United States of America, 2000.

[30] J. S. Milne , *Algebraic Number Theory*, Lecture notes for a course given at the University of Michigan, Ann Arbor, http://www.jmilne.org/math/coursenotes/.

[31] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers.* Springer, Berlin, 1980.

[32] P. Ribenboim, *Classical Theory of Algebraic Numbers* Springer, New York, 2001.

[33] S. Perlis, *Maximal Orders in Rational Cyclic algebras of composite degree*, in *Transactions of the American Mathematical Society*,vol.46, n.1, pp. 82-96, July 1939.

[34] PARI/GP, version `2.2.12`, Bordeaux, 2005, http://pari.math.u-bordeaux.fr.